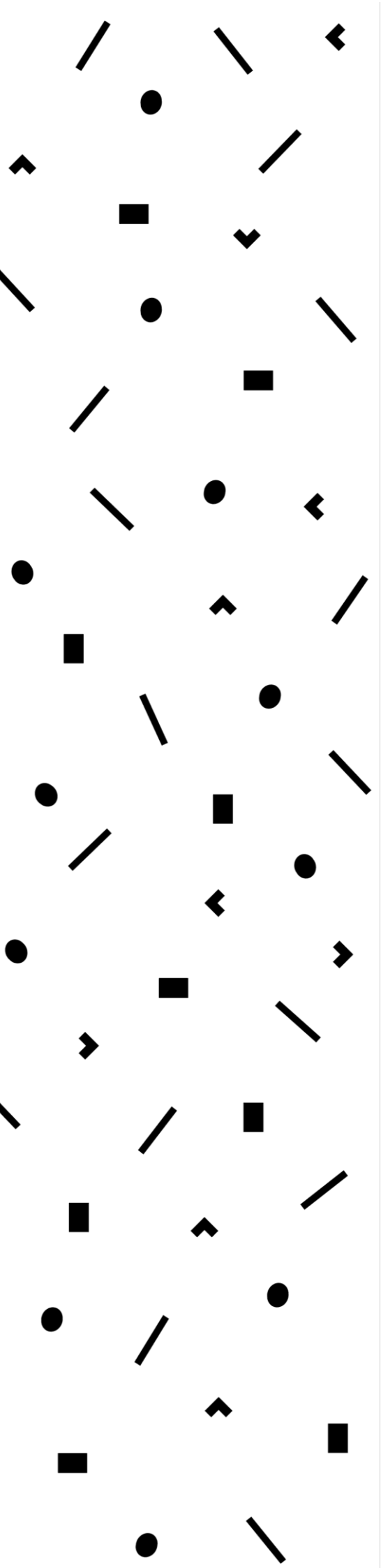


LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

PK-YRITYKSEN PALOMUURIRATKAISU

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2015
Samuli Peltola

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

PELTOLA, SAMULI: Pk-yrityksen palomuuriratkaisu

Tietoliikennetekniikan opinnäytetyö, 45 sivua

Kevät 2015

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli tutkia pk-yrityksille sopivia palomuuriratkaisuja. Palomuureista tutkittiin kahta avoimeen lähdekoodiin perustuvaa ratkaisua: pfSenseä ja VyOS:ia. Näiden lisäksi perehdyttiin Zyxell Zywall USG 300 -palomuurilaitteeseen.

Pk-yrityksissä tapahtuvan verkkoliikenteen määrä on lisääntynyt huomattavasti pilvipalvelutyyppisten sovellusten yleistyttyä. Tämän myötä palomuureiltakin vaaditaan parempia ominaisuuksia kuin aiemmin. Pk-yritykset ovat tutkimusten mukaan verkkohyökkäyksille otollisimmat kohteet, sillä niiden tietoturva ei ole yhtä korkealla tasolla kuin suuryrityksillä.

Palomuuri toimii tarkastuspisteenä kahden eri verkon välillä tapahtuvassa tietoliikenteessä. Palomuurin avulla pystytään hallitsemaan, mitkä paketit kulkevat mihinkin suuntaan vai estetäänkö ne. Perinteisen pakettien hallinnan lisäksi palomuureilla on QoS, jonka avulla rajoitetaan ja priorisoidaan verkkoliikennettä. Nykyaikaisten palomuurien avulla pystytään verkkoliikenteen hallinnan lisäksi luomaan VPN-yhteyksiä. VPN-yhteyksiä on kahta eri tyyppiä: site-to-site ja remote-access. Site-to-site VPN -tunnelin avulla pystytään yhdistämään kaksi verkkoa, esimerkiksi yrityksen pääkonttori ja sivukonttori. Remote-access-tyyppisen VPN-yhteyden avulla yrityksen työntekijä pystyy ottamaan internetin välityksellä yhteyden yrityksen verkkoon mistä päin maailmaa tahansa.

Tässä työssä vertaillaan kolmea palomuuriratkaisua, jotka ovat pfSense, VyOS ja Zyxell Zywall USG 300. Vertailussa päädyttiin siihen, että pfSense ja Zyxell Zywall USG 300 ovat sopivia pk-yrityksen tarpeisiin. VyOS:sta puuttuu IDS-järjestelmät ja graafinenkäyttöliittymä, minkä vuoksi sitä on hankalampi hallita.

Asiasanat: tietoturva, palomuuri, VPN, sisällönsuodatus, vikasietoisuus, pk-yritys

Lahti University of Applied Sciences
Degree Programme in Information Technology

PELTOLA, SAMULI: Firewall solution for small and medium-sized enterprises

Bachelor's Thesis in Telecommunications, 45 pages

Spring 2015

ABSTRACT

The goal of this thesis was to study firewall solutions for small to medium-sized enterprises. Three different solutions were studied and those were pfSense, VyOS and Zyxel Zywall USG 300.

The amount of network traffic in small to medium-sized enterprises has drastically increased after cloud computing became popular. Because of this the enterprises demand much more from their firewalls. Recent studies have revealed that small to medium enterprises are the easy targets for cyber-criminals, because they do not have enough good information security plans.

A Firewall works as a checkpoint between two different networks. It can be used to control packet flow, that is, whether packets are dropped, allowed or rejected. Modern firewalls have Quality of Service features which are used to shape network traffic. Firewalls also have VPN capabilities and they usually support two types of VPN connections, which are site-to-site and remote-access. Site-to-site is used to connect two different networks over the internet. Remote-access VPN is used when an employee wants to connect to a company network over the internet.

pfSense and Zyxell Zywall USG 300 were found the most suitable for small to medium-sized enterprises. VyOS was lacking a graphical user interface, which makes configuring and maintaining harder. Also VyOS did not have any kind of Intrusion Detection System.

Key words: information security, firewall, VPN, content filtering, failover, SME

SISÄLLYS

1 JOHDANTO

Tämän työn tarkoituksena on selvittää, minkälainen palomuuri on sopiva pk-yritykselle. Työssä perehdytään palomuurien toimintaan ja niiden ominaisuuksiin.

Pk-yrityksissä käytettävät ohjelmistot ovat tätä nykyä yhä useammin pilvipalvelu-tyyppisiä. Pilvipalvelu-tyyppisten ohjelmistojen kehittymisen ja internet-yhteyksien nopeuksien kasvaessa ovat pk-yritysten palomuureilta haluttavat ominaisuudet nousseet aivan uudelle tasolle. Tämän myötä markkinoille tulee jatkuvasti uusia valmiita palomuurilaitteita.

Työn tavoitteena on selvittää, mikä vertailluista laitteista on sopivin pk-yrityksen tarpeille. Suuri osa nykypäivän markkinoilla olevista palomuurilaitteista vaatii syvempää tietoliikenneteknistä osaamista, jotta niitä voidaan konfiguroida ja ylläpitää. Pk-yrityksillä ei välttämättä ole resursseja, joilta löytyy tätä vaadittua osaamista. Mahdollisen puuttuvan osaamisen vuoksi tässä työssä painotetaan laitteen helppokäyttöisyyttä.

Työn alkuosassa perehdytään siihen, miksi pk-yrityksissä tarvitaan tietoturvaa ja mitkä ovat pk-yritysten tietoturvan ongelmakohdat. Tutkimusosassa perehdytään palomuurien ominaisuuksien toimintaan. VPN-yhteydet ovat yleistyneet vihreän ICT-ajattelun myötä, sillä ne mahdollistavat etätyöskentelyn. Palomuurien vertailun jälkeen käydään läpi työn yhteenveto.

2 PK-YRITYKSEN TIETOTURVA

2.1 Pk-yrityksen tietoturva yleisesti

Kyberrikollisuus on moninkertaistunut viime vuosina. Vuonna 2008 Suomen poliisin tietoon tuli vain viisi tietomurtoa, kun taas vuonna 2014 määrä oli jo 368. Yhteensä vuonna 2014 poliisin tietoon tulleita tapahtuneita tietomurtoja, tietovuotoja, henkilörekisteririkoksia ja muita kyberrikoksia oli 1251 kappaletta. Yli puolet näistä rikoksista jää selvittämättä. (Yle 2015.)

Pk-yritys on usein otollisin kohde kyberrikolliselle. Suuryrityksillä on paljon resursseja, joiden avulla kyberrikollisia kiinnostavat tiedot ovat suojattuna, kun taas tavallisella kuluttajalla tai pienyrityksellä ei useimmiten ole kyberrikollisia kiinnostavia tietoja. (Check Point 2013.)

Pk-yrityksillä on usein tarpeeksi kyberrikollisien havittelemaa arvokasta tietoa ja suhteellisen heikko tietoturva verrattuna suuryrityksiin. National CyberSecurity Alliancen (NCSA) vuoden 2012 pk-yritysten tietoturvatutkimuksen mukaan 90 % tutkimukseen osallistuneilta pk-yrityksiltä puuttui tietohallintopäällikkö ja tietoturvaan erikoistuneita henkilöitä oli vielä vähemmän. (Check Point 2013.)

2.2 Pk-yrityksen tietoturvan ongelmat

NCSA:n tutkimuksen mukaan 50 % pk-yrityksistä uskoo olevansa liian pieniä kiinnostaaksensa kyberrikollisia. Pk-yrityksissä uskotaan tietoturvan olevan liian kallista ja monimutkaista. (Check Point 2013.)

Epäonnistumalla tietoturvauhkien torjunnassa suuri tietomurto tai tietovuoto voi pahimmillaan aiheuttaa yritykselle konkurssin. The Wall Street Journal julkaisi 2013 maaliskuussa tutkimuksen, jonka mukaan suurin osa pk-yrityksistä ei pystyisi palautumaan tietomurrosta. Silti suuressa osassa yrityksiä ei uskota potentiaaliseen uhkaan tai luullaan

yrityksen tietoturvan olevan jo tarpeeksi korkealla tasolla. (Check Point 2013.)

2.3 Pk-yrityksen tietoturvan edut

Yksinkertaisin tapa toteuttaa tietoturvaa Pk-yrityksessä on palomuurin käyttöönotto. Pk-yrityksissä hyvin toteutettu tietoturva tukee liiketoimintaa esimerkiksi seuraavin tavoin:

- Pystytään jakamaan tietoa yhteistyökumppaneiden kanssa antamalla heille rajattu pääsy verkkoon.
- Verkon häiriötilanteiden määrä saadaan minimoitua.
- Mahdollistaa etäyhteyden avulla työskentelyn mistä vain.
- Pienentää tietomurron ja tietovuodon riskiä.

(Cisco 2015.)

3 PALOMUURI

3.1 Palomuurit yleisesti

Palomuuri on tarkastuspiste kahden eri verkon välillä tapahtuvaa tietoliikennettä varten. Useimmiten palomuuri on kuitenkin internetin ja yksityisen verkon välissä tarkkailemassa tietoliikennettä. Palomuurin tehtävänä on joko sallia (pass), estää (drop) tai hylätä (reject) tuleva ja lähtevä liikenne, konfiguroitujen sääntöjen mukaisesti. Jos palomuuri on oikein konfiguroitu ja palomuurin ohjelmisto ei sisällä tietoturva-aukkoja, on palomuurin suojaama verkko turvattuna ulkoisilta uhilta niin hyvin kuin mahdollista. (Strebe & Perkins 2002, 3.)

Palomuureja on kahta eri tyyppiä: laitepalomuureja ja ohjelmapalomuureja. Ohjelmapalomuurit ovat loppukäyttäjän työasemaan tai serveriin asennettuja ohjelmia. Ne toimivat yleensä ISO OSI -mallin (International Organization for Standardization Open Systems Interconnection Reference Model) (kuvio 1) kolmannella ja neljännellä kerroksella. (Frahim, Santos & Ossipov 2014, 2 - 3, 9.)

OSI-mallin 7 kerrosta	
7. Sovelluskerros (Application Layer)	HTTP,FTP,SMTP
6. Esitystapakerros (Presentation Layer)	JPEG, GIF, ASCII
5. Istuntokerros (Session Layer)	RPC, SQL, NFS
4. Kuljetuskerros (Transport Layer)	TCP/SPX/UDP
3. Verkkokerros (Network Layer)	IP/IPX/ICMP
2. Siirtokerros (Data Link Layer)	MAC-osoitteet, PPP, SLIP
1. Fyysinen kerros (Physical Layer)	Verkkokaapelit, kytkimet

KUVIO 1. ISO OSI -malli

Hyvä palomuuri toimii jokaisella ISO OSI -mallin kerroksella siirtokerroksesta sovelluskerrokseen. Palomuureissa on pääsääntöisesti kolme perustoimintoa:

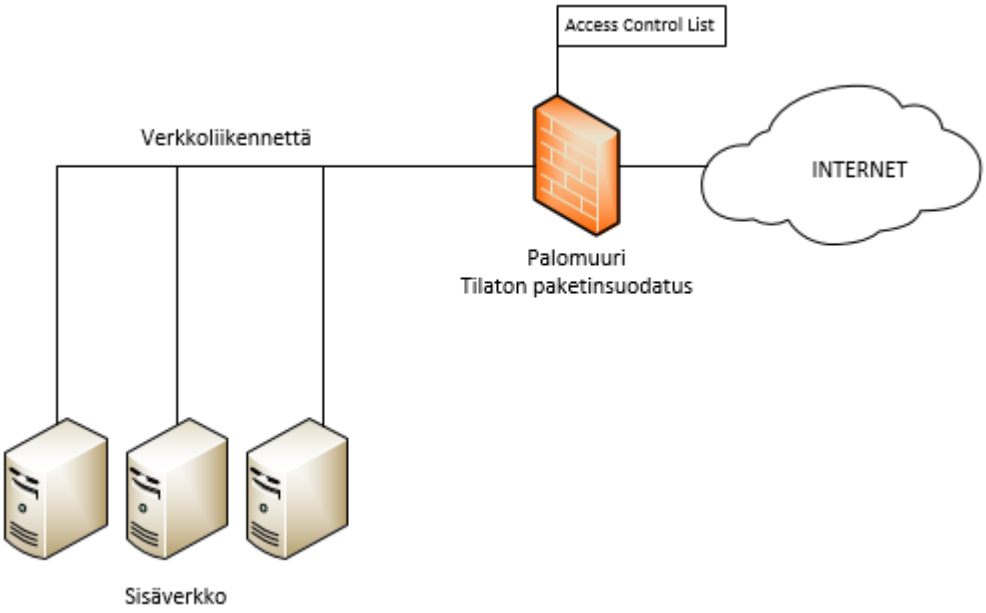
- pakettien suodatus, hylkää TCP/IP (Transmission Control Protocol / Internet Protocol) -paketit auktorisoimattomilta lähettäjiltä
- NAT (Network Address Translation), piilottaa sisäverkon laitteiden IP-osoitteet (Internet Protocol address) ulkoverkolta
- välityspalvelin eli proxy-palvelu, proxy-palvelun tehtävänä on mahdollistaa kahden isäntäkoneen epäsuora kommunikointi keskenään.

Näiden toimintojen lisäksi suurin osa palomuureista tukee myös lokitusta, salattua autentikaatiota ja VPN-ratkaisuja (Virtual Private Network). Moderneista palomuureista löytyy myös Intrusion Detection System (IDS). (Strebe & Perkins 2002 4.)

3.2 Palomuurien ominaisuudet

3.2.1 Paketinsuodatus

Paketinsuodattimen tarkoitus on kontrolloida pääsyä tiettyihin verkon segmentteihin määrittelemällä, mikä liikenne pääsee suodattimen läpi. Yleensä paketinsuodattimet tutkivat liikennettä ISO OSI -mallin kuljetuskerroksella.



KUVIO 2. Tilaton palomuuri

Esimerkiksi tilattomien palomuurien paketinsuodattimet (kuvio 2) voivat analysoida TCP- tai UDP (User Datagram Protocol) -paketteja ja verrata niiden sisältöä Access Control List (ACL) -pääsylistoihin. Suodattimet tutkivat paketeista seuraavia ominaisuuksia:

- lähdeosoitetta
- kohdeosoitetta
- lähdeporttia
- kohdeporttia
- protokollaa.

Useat paketinsuodattimet pystyvät tämän lisäksi tutkimaan paketin header- eli otsikkotietoja, joiden avulla selviää, onko tutkittava paketti uudesta vai jo auki olevasta yhteydestä peräisin. Paketinsuodatusta suorittavan tilattoman palomuurin suurimpia ongelmia ovat pääsylistojen hallittavuus ja ohjelmat, jotka ottavat useita yhteyksiä sattumanvaraisiin portteihin. Tällaisia ohjelmia ovat esimerkiksi monet kuvan ja äänen suoratoisto-ohjelmat. Paketinsuodattimet eivät ymmärrä tällaisten ohjelmien käyttämiä ylemmän kerroksen protokollia, koska pääsylistat konfiguroidaan manuaalisesti. (Frahim ym. 2014, 2 - 3.)

Tilattomien palomuurien lisäksi markkinoilla on tilallisella paketinsuodatuksella varustettuja SPI (Stateful Packet Inspection) -palomuureja. Tilallisen paketinsuodatuksen suurin etu verrattuna tilattomaan on tilallisen paketinsuodatuksen kyky tarkastaa, kuuluuko paketti jo avoinna olevaan yhteyteen. Jos tutkittu paketti kuuluu jo auki olevaan yhteyteen, paketti päästetään läpi. Uutta yhteyttä avattaessa tilallinen palomuuri katsoo, onko yhteys sallittu palomuurin sääntöjen perusteella. Jos yhteys on sallittu, lisätään kyseinen yhteys palomuurin yhteyslistaan ja tulevaisuudessa kaikki kyseisen yhteyden paketit päästetään läpi. Yhteyden sulkeutuessa tai yhteyden oltua tarpeeksi kauan inaktiivinen, poistaa palomuuri kyseisen yhteyden sallittujen yhteyksien listalta ja sulkee yhteyden käyttämät portit. (Check Point 2005, 7.)

3.2.2 Network Address Translation

Network Address Translation (NAT) eli osoitteenmuunnos on ominaisuus, joka löytyy lähes jokaisesta palomuurista. Alun perin NAT kehitettiin IP-osoitteiden säästämistä varten, sillä IPv4 (Internet Protocol version 4) tukee vain noin 4:ää miljardia IP-osoitetta. NAT:n avulla kaikki sisäverkon laitteet voivat käyttää yksityisiä IP-osoitteita, jotka eivät ole käytössä internetissä (kuvio 3).

RFC 1918 Yksityisten IP-osoitteiden alueet	
IP-osoite alue	Verkko/Maski
10.0.0.0-10.255.255.255	10.0.0.0/8
172.16.0.0-172.31.255.255	172.16.0.0/12
192.168.0.0-192.168.255.255	192.168.0.0/16

KUVIO 3. Yksityiset IP-osoitteet

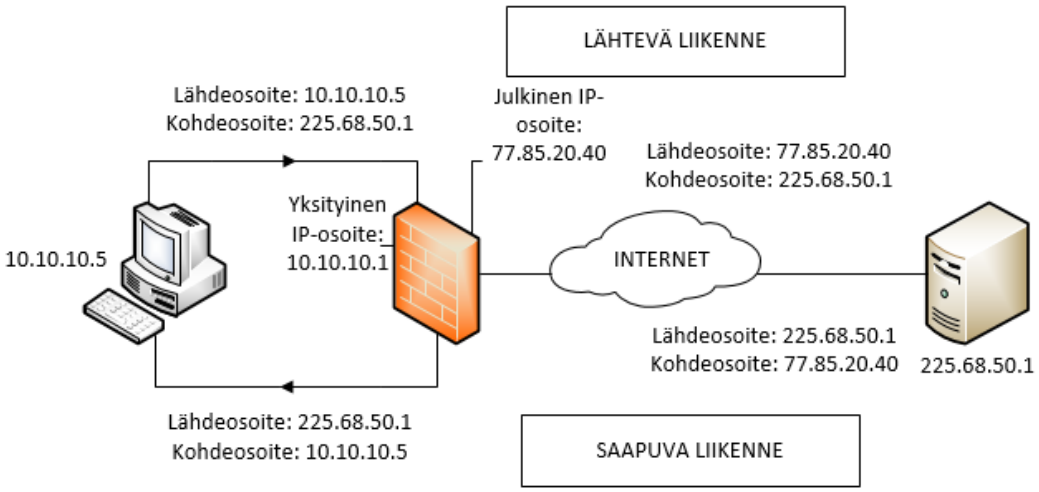
Osoitteenmuunnoksia on kolmea eri tyyppiä: staattinen NAT, dynaaminen NAT ja NAT overloading, joka tunnetaan myös nimellä PAT (Port Address Translation). Staattista NAT käytetään silloin, kun tietyn verkon resurssin

täytyy olla saatavilla ulkoverkosta. Staattisessa NAT:ssa on ennalta määritelty, mikä osoite muuttuu miksikin. (Frahim ym. 2014, 3 - 6.)

Dynaamisessa NAT:ssa ulkoverkolla on tietty julkisten IP-osoitteiden alue. Dynaaminen NAT muuntaa sisäverkon osoitteen ensimmäiseksi vapaaksi julkisen IP-osoitealueen osoitteeksi. Tällöin sisäverkon laitteet voivat ulkoverkossa näkyä millä tahansa ennalta määritellyn julkisen osoitealueen osoitteella. (Strebe & Perkins 2002, 154 - 155.)

PAT:ssa useat sisäverkon laitteet jakavat saman julkisen IP-osoitteen. Tällöin sisäverkon laitteet erotellaan hyödyntämällä IP-osoitteen lisänä TCP- ja UDP-pakettien header-tiedosta löytyviä porttinumeroita. (Frahim ym. 2014, 4 - 5.)

NAT käytettäessä sisäverkon laitteen yhdistäessä internetiin, paketin lähdeosoitteena näkyy yksityinen IP-osoite. Osoitteenmuunnoksen tekevä laite muuttaa paketin lähdeosoitteeksi oman julkisen IP-osoitteensa, jolloin internetissä oleva vastaanottava laite luulee paketin tulleen osoitteenmuunnoksen tehneeltä laitteelta (kuvio 4).



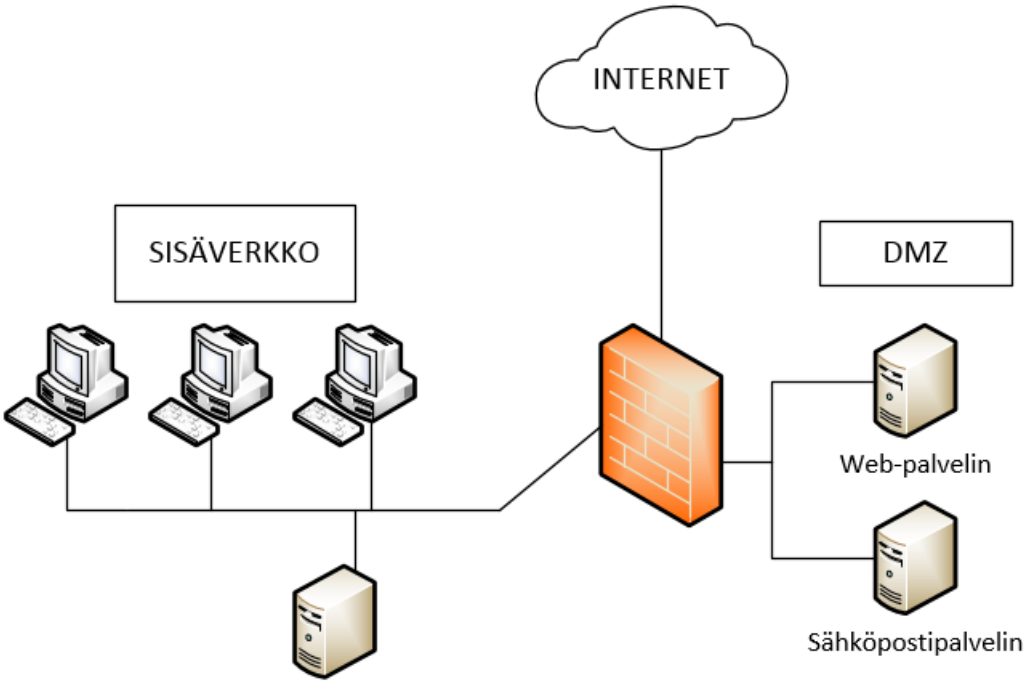
KUVIO 4. Network Address Translation käytännössä

Internetissä sijaitseva laite taas vastaa kyseiseen pakettiin asettamalla kohdeosoitteeksi osoitteenmuunnoksen tehneen laitteen julkisen IP-osoitteen. Osoitteenmuunnoksen jälkeen paketin kohdeosoitteeksi vaihtuu

taas sisäverkon IP-osoite. NAT-laite pitää listaa, mitkä IP-osoitteet pitää muuttaa miksikin. Tällaista listaa kutsutaan NAT-tauluksi. (Komar, Beekelaar & Wettern 2003, 62 - 63.)

3.2.3 Demilitarized Zone (DMZ)

Palomuurit voidaan konfiguroida erottamaan segmenttejä sisäverkosta. Näitä erotettuja segmenttejä kutsutaan yleisesti nimityksellä demilitarized zone. DMZ-alueella olevat laitteet voivat muodostaa suoria yhteyksiä muihin saman alueen laitteisiin ja ulkoverkkoon, mutta eivät sisäverkkoon. Yleensä palomuuri kuitenkin rajoittaa tietoturvasyistä suoria yhteyksiä DMZ:lta ulkoverkkoon. Yksinkertaisimmin DMZ:n voi toteuttaa palomuurilla, jossa on kolme verkkoliitäntää. Tällöin yksi liitäntä on sisäverkolle, yksi DMZ:lle ja yksi ulkoverkolle (kuvio 5).



KUVIO 5. Yhden palomuurin ja DMZ:n konfiguraatio

Demilitarized Zonelle sijoitetaan yleensä sellaisia palvelimia ja palveluita, joiden täytyy olla saatavilla ulkoverkossa. Tällainen tilanne on esitetty kuviossa 5. Sähköpostipalvelin vastaanottaa viestit internetistä, välittää ne sisäverkkoon ja välittää sisäverkosta tulevat sähköpostit internetiin. Tämän

takia sähköpostipalvelin täytyy sijoittaa DMZ:lle. (Strebe & Perkins 2002, 22 - 23.)

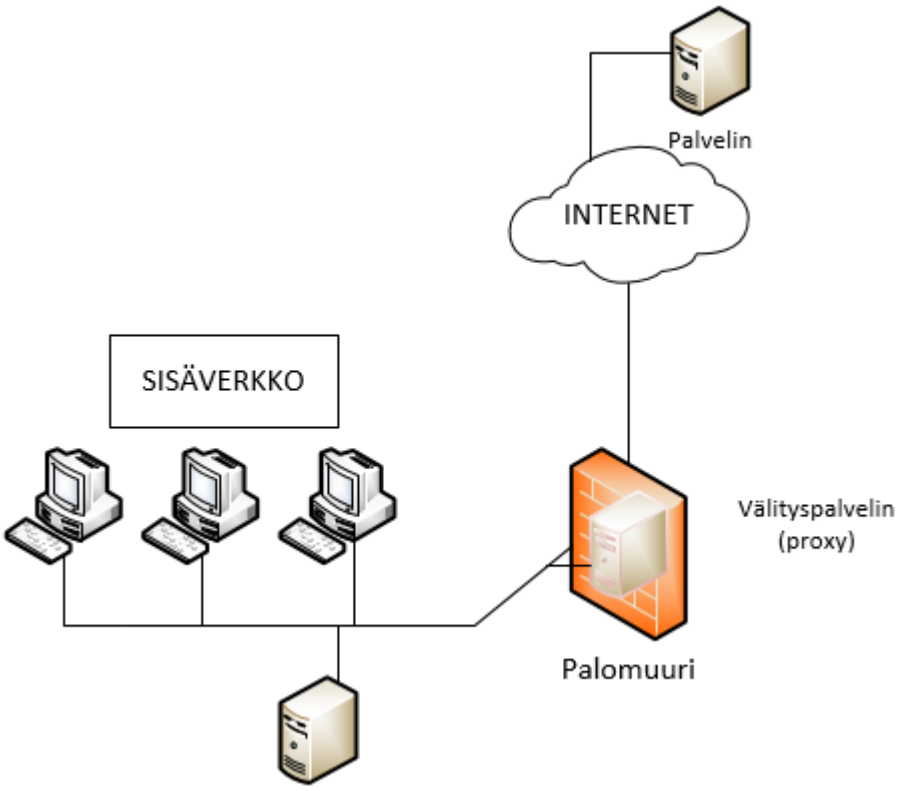
Suuryritysten verkoissa voi DMZ-segmenttejä ja palomuureja olla useita. Useaa eri DMZ-segmenttiä ja palomuuria käytettäessä pystytään määrittelemään jokaisen DMZ-segmentin tietoturva-asetukset erikseen ja näin koko verkon tietoturvallisuus kasvaa. (Komar ym. 2003, 200 - 203.)

3.2.4 Palomuuri välityspalvelimena

NAT ratkoo suurimman osan ongelmista, jotka liittyvät ulkoverkon yhteyksiin, mutta ei silti rajoita pakettien kulkua palomuurin läpi. Hakkerit voivat tarkkailla verkon monitorointiin suunnitelluilla työkaluilla verkkoliikennettä ja päätellä verkkoliikenteen perusteella palomuurin suorittavan osoitteenmuunnoksia. Tämä tieto mahdollistaa hakkereille TCP-yhteyden kaappaamisen tai väärentämisen. Kaapatulla tai väärennetyllä TCP-yhteydellä hakkeri pystyy muodostamaan yhteyden palomuurin läpi ja samalla pääsee käsiksi palomuurin suojaamaan sisäverkkoon. (Strebe & Perkins 2002, 11 - 12.)

Välityspalvelimena toimivasta palomuurista käytetään nimitystä sovellustason välityspalvelin (application-level proxy). Sovellustason välityspalvelimien avulla pystytään katkaisemaan palomuurin läpi kulkeva verkkokerroksen pakettivirta ja rajoittaa liikenne ainoastaan tiettyihin korkeamman tason protokolliin, kuten HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol) ja SMTP (Simple Mail Transfer Protocol). (Strebe & Perkins 2002, 11 - 12.)

Välityspalvelin odottaa sisäverkosta tulevaa ulkoverkkoon kohdistuvaa yhteyttä ja kaappaa yhteyden. Tämän jälkeen välityspalvelin ottaa yhteyden ulkoverkon kohteeseen sisäverkon laitteen sijaan, eli välityspalvelimena toimiva laite suorittaa eräänlaisen man-in-the-middle-hyökkäyksen (kuvio 6). (Strebe & Perkins 2002, 11 - 12.)



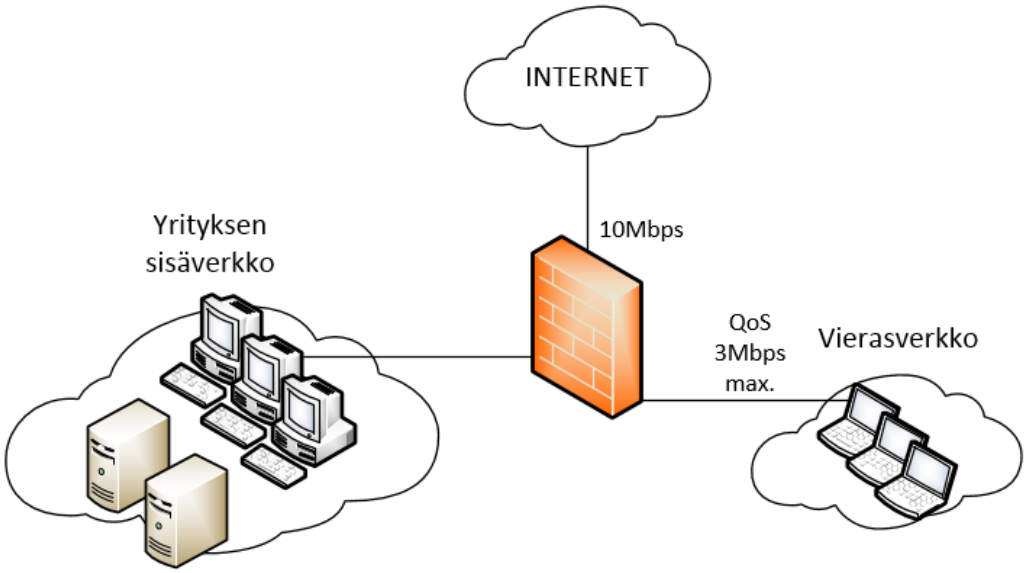
KUVIO 6. Palomuuri välityspalvelimena

Palomuurin ei ole pakko toimia sovellustason välityspalvelimena vaan välityspalvelimena voi toimia mikä tahansa palvelin, sisäverkossa tai ulkoverkossa. Kuitenkaan ilman palomuuria sisäverkko ei ole turvassa, joten tietoturvallisesta verkosta löytyvät molemmat. Jos palvelin toimii sovellustason välityspalvelimena, täytyy palomuurin suojata sitä vähintään paketinsuodattimen avulla. Ilman paketinsuodatusta proxy-palvelin on alttiina palvelunestohyökkäyksille (denial-of-service attack). (Strebe & Perkins 2002, 11 - 12.)

3.2.5 QoS eli Quality of Service

Verkon QoS tarkoittaa palomuurin läpi kulkevan liikenteen priorisointia. Usein puhutaan myös traffic shapingista. Ilman traffic shapingia palomuuri käsittelee paketteja first in/first out -periaatteella, eli ensimmäisenä palomuurille tullut paketti lähtee ulos ensimmäisenä riippumatta paketin sisällöstä. QoS:n avulla voidaan priorisoida erityyppistä liikennettä ja varmistaa, että alhaisen prioriteetin palvelut eivät käytä kaikkea saatavilla

olevaa kaistaa ja näin estä tärkeiden palvelujen toimintaa. Yleensä QoS:lla varmistetaan yrityksissä kriittisten palveluiden, kuten toiminnanohjausjärjestelmien, VoIP-puheluiden (Voice over Internet Protocol) ja videoneuvottelujen toimivuus. Eri protokollien priorisoinnin lisäksi voidaan rajoittaa tiettyjen verkkoliitäntöjen nopeutta. Esimerkkinä kuviossa 7 näkyvä tilanne, jossa vierasverkko on liitetty palomuurin eri verkkoliitäntään kuin yrityksen varsinainen lähiverkko. Ilman QoS:a vierasverkon käyttäjä pystyisi tukkimaan yrityksen koko internet-yhteyden. (Buechler & Pingle 2009, 326.)



KUVIO 7. Vierasverkon nopeus rajoitettu

3.2.6 Virtual Private Network (VPN) yleisesti

Nykypäivän palomuureista löytyy lähes poikkeuksetta tuki VPN-ratkaisuille. VPN-ratkaisu tarjoaa yritykselle keinon varmistaa tietojen eheys, kryptata tiedot ja tavan autentikoida lähetettäessä paketteja suojaamattomassa verkossa tai internetissä. VPN-ratkaisut suunniteltiin alun perin korvaamaan leased line tyyppisiä vuokrattuja yhteyksiä. (Dell Software 2013.)

VPN-ratkaisuissa käytetään useita eri protokollia, esimerkiksi seuraavia:

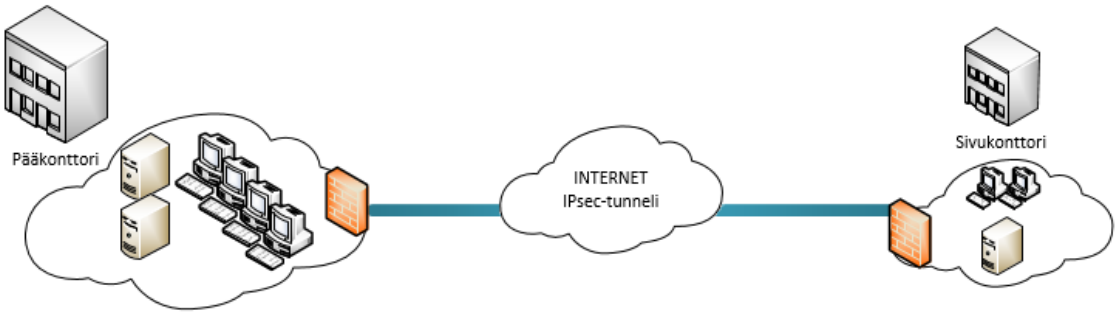
- Point-to-Point Tunneling Protocol (PPTP)

- Layer 2 Forwarding Protocol (L2F)
- Layer 2 Tunneling Protocol (L2TP)
- Generic Routing Encapsulation Protocol (GRE)
- Multiprotocol Label Switching (MPLS) VPN
- Internet Protocol Security (IPsec)
- Secure Sockets Layer (SSL).

Näistä protokollista L2F, L2TP, GRE ja MPLS VPN eivät tue tietojen varmennusta, autentikaatiota ja tietojen kryptausta. IPsec voidaan yhdistää kyseisten protokollien kanssa korvaamaan niiden tietoturvapuutteet. Nykypäivänä site-to-site VPN-tunneleissa käytetyin protokolla on IPsec, sillä IPsec tukee kaikkia turvalliselta VPN-yhteydeltä vaadittavia tietoturvaominaisuuksia. Remote-access-tyyppisissä VPN-ratkaisuissa taas käytetään useimmiten SSL-protokollaa. (Frahim ym. 2014, 14 - 15.)

VPN-ratkaisut voidaan jakaa kahteen osaan: site-to-site-tyyppisiin VPN-yhteyksiin ja remote-access VPN-yhteyksiin. Nykyaikaiset palomuurit tukevat kummankin tyyppisiä ratkaisuja. (Frahim ym. 2014, 15.)

Site-to-site-tyyppisellä VPN-yhteydellä pystytään luomaan VPN-tunneli kahden eri verkon välille käyttäen internetiä verkot yhdistävänä käytävänä. Tyypillisesti Site-to-site VPN-tunneli rakennetaan kahden (kuvio 8) tai useamman tietoliikenneverkkolaitteen välille. (Frahim ym. 2014, 15.)



KUVIO 8. Sivukonttori yhdistettynä pääkonttoriin IPsec-tunnelilla

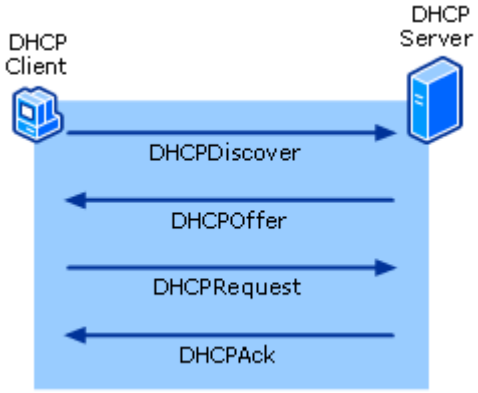
Remote-access VPN-ratkaisussa käyttäjä voi ottaa yhteyden yrityksen verkkoon omalta päätelaitteeltaan mistä päin maailmaa tahansa, jos vain

internet-yhteys on saatavilla. Remote-access VPN-ratkaisua voidaan käyttää myös, jos halutaan antaa yhteistyökumppaneille rajattu oikeus yhdistää yrityksen suojattuun verkkoon. (Dell Software 2013.)

3.2.7 Dynamic Host Configuration Protocol

DHCP on protokolla, jonka tehtävä on jakaa verkkoon kytkeytyville laitteille IP-osoite, aliverkon peite (subnet mask), oletusyhdyskäytävän osoite (default gateway) ja mahdollisesti nimipalvelimen osoite (Domain Name System) (DNS). Jakamisen suorittaa aina DHCP-serveri, jolle on määritelty saatavilla oleva IP-osoitealue. (Microsoft 2003.)

Osoitteen haluava päätelaite lähettää verkkoon DHCPDiscover-viestejä 0, 4, 8, 16 ja 32 sekunnin välein. Jos päätelaite ei saa vastausta minuutin aikana, päätelaite ottaa joko Automatic Private IP Addressing (APIPA) mukaisen itse konfiguroidun IP-osoitteen verkkoliitynnälleen. Vaihtoehtoisesti, jos päätelaite ei tue APIPA:a tai IP-osoitteen automaattinen konfigurointi on disabloitu, asiakasohjelman verkkoon liittyminen epäonnistuu. DHCP-serveri vastaa päätelaitteen DHCPDiscover-viestiin DHCPOffer-viestillä, jossa tarjotaan IP-osoitetta. Tämän jälkeen päätelaite hyväksyy IP-osoitteen ja lähettää DHCP-serverille DHCPRequest-viestin, jonka serveri kuittaa DHCPAck-viestillä. Tämän prosessin päätteeksi DHCP-palvelimelta on varattu yksi IP-osoite, osoitetta pyytäneelle päätelaitteelle. Kuviossa 9 on kuvattuna DHCP-palvelun prosessi. (Microsoft 2003.)



KUVIO 9. DHCP-palvelimelta osoitteen haku (Microsoft 2003)

DHCP-relay on palvelu, joka kuuntelee DHCP broadcast -viestejä aliverkossa ja ohjaa ne DHCP-serverille. DHCP-serveri taas lähettää vastauksen DHCP-relayna toimivalle laitteelle ja DHCP-relay toimittaa vastauksen oikeaan osoitteeseen. Ilman DHCP-relay-palvelua, jokaisessa aliverkossa täytyisi olla DHCP-serveri vastaamassa DHCP-kyselyihin. DHCP-relayn avulla siis pystytään keskittämään DHCP-osoitteiden hallinta. (Microsoft 2003.)

3.2.8 High Availability

Ympärivuorokautinen verkon toiminta on yksi nykypäivän yritysten kulmakivistä. Kaikki verkon häiriöaika johtaa suoraan rahallisiin tappioihin ja pahimmassa tapauksessa vahingoittaa yrityksen brändiä. Tämän takia useimmissa nykypäivän palomuureissa on High Availability (HA) -ominaisuuksia, jotka pyrkivät minimoimaan verkon häiriöajan. Yleisimpiä HA-ominaisuuksia ovat seuraavat:

- redundanttiset verkkoliitynnät
- vikasietoisuus
- klusterointi.

Redundanttisilla verkkoliitynnöillä tarkoitetaan yleensä kahden verkkoliitynnän pariuttamista, jolloin vain yksi fyysinen verkkoliityntä on toiminnassa. Tällöin toinen liityntä on valmiustilassa ja odottaa käytössä olevan liitynnän vikaantumista. Yleensä redundanttisten verkkoliityntöjen pareilla on konfiguroituna virtuaaliset MAC-osoitteet. Liitynnän vikaantuessa vikaantuneen liitynnän virtuaalinen MAC-osoite siirretään valmiustilassa olevalle ja näin valmiustilassa oleva jatkaa vikaantunen liitynnän toimintaa. (Frahim ym. 2014, 642 - 643.)

Vikasietoisuus eli failover on vanhin HA:n muoto palomuureissa. Failover tarkoittaa yksinkertaisesti sitä, että kun yksi laite vikaantuu, toinen ehjä ja identtinen laite ottaa vikaantuneen laitteen roolin. (Frahim ym. 2014, 652.)

Klusteroinnilla tarkoitetaan palomuureissa yleensä kahden tai useamman palomuurilaitteen konfiguroitua tilaa, jossa käytössä olevan laitteen vikaannuttua, ehjä laite ottaa vikaantuneen paikan. Normaalitilassa kaikki klusteriin kuuluvat laitteet toimivat yhdessä jakaen tehtävät. (Frahim ym. 2014, 685.)

4 IPSEC JA SSL VPN-YHTEYDET

4.1 IPsec VPN

IPsec-yhteydet toimivat OSI-mallin kolmannella- eli verkkokerroksella. Tästä syystä IPsec-tunnelissa tieto matkaa tunnelin muodostavien laitteiden välillä ilman minkään sovelluksen osallistumista. Kun IPsec-tunneli on muodostettu, kaikki tunnelin muodostavien verkkolaitteiden takana olevat resurssit ovat auki tunnelin molempiin päihin.

IPsec käyttää Internet Key Exchange (IKE) -protokollaa neuvotellessaan ja muodostaessaan site-to-site- ja remote-access-tyyppisiä VPN-tunneleita. IKE koostuu ISAKMP- (Internet Security Association and Key Management Protocol), Oakley- ja SKEME (Secure Key Exchange Mechanism) -protokollista. IKE:ssä on kaksi vaihetta, ja siitä on kaksi eri versiota: IKEv1 ja IKEv2. (Frahim ym. 2014, 16.)

IKEv1 ensimmäisessä vaiheessa muodostetaan IPsec tunnelin muodostavien laitteiden välille tietoturvallinen ja kaksisuuntainen yhteys, josta käytetään nimitystä ISAKMP Security Association (SA). IKE:n ensimmäisessä vaiheessa päätelaitteet vaihtavat UDP-porttia 500 seuraavat tunnelin muodostuksessa käytettävät tiedot keskenään:

- salausalgoritmi
- tiiviste algoritmi eli hash algoritmi
- autentikointitapa
- Diffie-Hellman ryhmä.

(Frahim ym. 2014, 16. 18 - 20.)

IKEv1 toisessa vaiheessa (quick mode) tunnelia muodostavat laitteet neuvottelevat, ensimmäisessä vaiheessa luodun yhteyden avulla, SA:t IPsecin ja muiden puolesta. Toisen vaiheen neuvotteluista muodostuu aina vähintään kaksi yksisuuntaista Security Associationia: toinen saapuvalle liikenteelle ja toinen lähtevälle. (Carrel & Harkins 1998.)

IKEv2 toi useita parannuksia versioon yksi verrattuna. Näistä oleellisimmat ovat seuraavat:

- IKEv2 käyttää vähemmän kaistaa kuin IKEv1.
- IKEv2 havaitsee, onko tunneli vielä elossa, IKEv1 ei.
- IKEv2:ssa on sisäänrakennettu NAT-T (Network Address Translation Traversal), jonka avulla IKEv2 pystyy neuvottelemaan osoitteenmuunnoksesta huolimatta.
- IKEv2 tukee EAP-protokollaa (Extensible Authentication Protocol).

(Kaufman 2005.)

Yleisimpiä IPsec-tunneleissa käytettäviä salausalgoritmeja ovat Data Encryption Standard (DES), Triple DES (3DES) ja Advanced Encryption Standard (AES). Tiiviste algoritmeista taas yleisimmät ovat Secure Hash Algorithm (SHA) ja Message digest algorithm 5 (MD5). Pk-yritykset ja sitä pienemmät käyttävät autentikointitapana useimmiten ennalta jaettuja avaimia (pre-shared key) (PSK). (Frahim ym. 2014, 18.)

IPsec:n avulla voidaan muodostaa site-to-site VPN-tunnelien lisäksi remote-access VPN-tunneleita. Remote-access-tyyppiset ratkaisut IPsecin avulla eivät kuitenkaan ole läheskään yhtä tietoturvallisia kuin SSL VPN, koska IPsec avaa aina koko verkon etäyhteyden muodostettua. Suurimmat remote-access SSL VPN:n edut verrattuna vastaavaan IPsec-ratkaisuun ovat SSL VPN -yhteyden helppo käytettävyys ja mahdollisuus rajata, mitä verkon resursseja etäyhteyden yli on saatavilla. IPsec VPN vaatii aina asiakasohjelman ja etäyhteyttä varten käyttäjä joutuu asentamaan kyseisen ohjelman. (Dell Software 2013.)

4.2 SSL VPN

SSL VPN käyttää SSL-protokollaa yhteyden muodostamiseen ja toimii OSI-mallin seitsemännellä, eli sovelluskerroksella. SSL-protokollasta käytetään nykyään nimitystä TLS (Transport Layer Security). Internet

Engineering Task Force (IETF) loi TLS:n yhdistääkseen eri SSL-versiot yhden avoimen standardin alle. (Cisco 2009.)

Kaikista suosituin sovellus, joka käyttää SSL-protokollaa, on http, World Wide Webin suuren suosion takia. Kaikki suosituimmat web-selaimet tukevat HTTPS:ää (HTTP over SSL/TLS). Käytettäessä SSL:ää VPN-yhteydessä saavutetaan vastaavanlainen tietojen suojauksen taso kuin IPsec:ssä. Koska suurin osa sovelluksista tukee SSL:ää, pystyy VPN-käyttäjä ottamaan yhteyden yritysverkon resursseihin mistä tahansa ja millä tahansa PC:llä. (Cisco 2009.)

SSL soveltuu yritysten remote-access VPN-ratkaisuihin erittäin hyvin, koska SSL VPN-yhteyden käyttäminen ei välttämättä vaadi asiakasohjelman asentamista. Samasta syystä yritysten VPN-ratkaisuun liittyvät pienenevät, mikä on suuri etu verrattuna IPsec-pohjaiseen ratkaisuun. (Cisco 2009.)

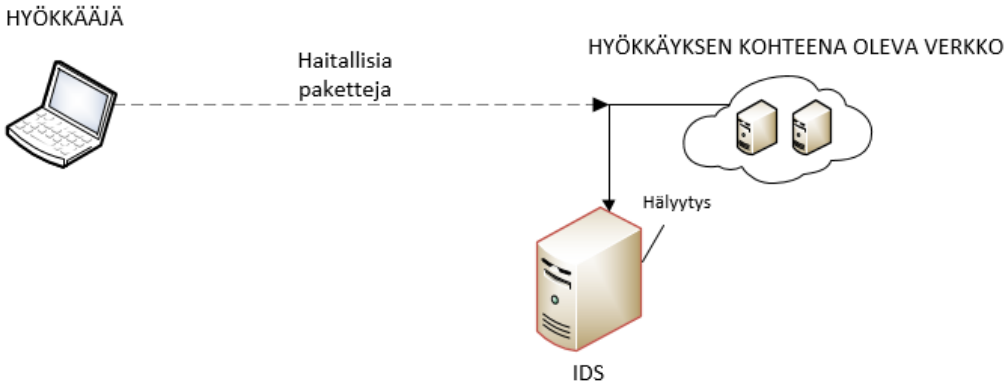
Suurimmat syyt SSL VPN:n suosioon ovat SSL VPN:n helppokäyttöisyys ja kyky rajata, mitä resursseja halutaan antaa etäyhteyden avaajalle. SSL VPN käyttää samaa TCP/443-porttia, kuin HTTPS ja tämän takia ei vaadi erillisiä konfiguraatiomuutoksia palomuuriin tai NAT:iin. IPsec taas käyttää IP protokollia 50 (ESP) (Encapsulation Security Payload), 51 (AH) (Authentication Header) ja täten vaatii palomuurin konfiguraatiomuutoksia. (Frahim ym. 2014, 24.)

IPsec vai SSL, kysymykseen ei ole yksioikoista vastausta. Molemmat protokollat toimivat hyvin nykyaikaisissa VPN-ratkaisuissa. IPsec toimii paremmin site-to-site-tyyppisissä ratkaisuissa, joissa halutaan pysyvästi yhdistää esimerkiksi yrityksen sivukonttori pääkonttoriin. SSL VPN -ratkaisut ovat taas IPsec-ratkaisuja parempia remote-access-tyylisissä ratkaisuissa, joissa yksittäinen käyttäjä ottaa etäyhteyden yrityksen verkkoon. (Cisco 2009.)

5 IDS JA IDP JÄRJESTELMÄT

5.1 Intrusion Detection System

Monessa nykypäivän palomuurissa on mukana tunkeilijan havaitsemisjärjestelmä, eli IDS. Tunkeilijan havaitsemisjärjestelmät ovat laitteita, jotka havaitsevat hyökkäyksiä, joiden avulla yritetään saada luvaton pääsy verkkoon tai päätelaitteeseen. Yleensä hyökkäyksillä halutaan lamauttaa tai heikentää hyökkäyksen kohteena olevan verkon suorituskykyä tai varastaa tietoa. IDS-järjestelmät pystyvät myös havaitsemaan palvelunestohyökkäyksiä ja viruksia. (Frahim ym. 2014, 9.)



KUVIO 10. IDS-järjestelmän toiminta

IDS-järjestelmä valvoo kuvion 10 mukaisesti verkkoon tulevia paketteja ja hälyyttää haitallisten pakettien saapuessa. IDS-järjestelmän heikkous on se, että haitallinen paketti pääsee kuitenkin verkkoon. (Frahim ym. 2014, 9.)

5.2 Intrusion Prevention System

Intrusion Prevention System eli tunkeilijan estojärjestelmä korjaa IDS-järjestelmän puutteen ja kykenee pudottamaan haitallisen paketin. Haitallisten pakettien pudottamisen lisäksi IPS-järjestelmä kykenee havaitsemaan samalla tavalla hyökkäyksiä, kuin IDS-järjestelmät.

IPS-järjestelmiä on kahta eri tyyppiä: verkkopohjaisia (Network-based Intrusion Prevention System) (NIPS) ja päätelaitepohjaisia (Host-based Intrusion Prevention System) (HIPS). Verkkopohjaiset IPS-järjestelmät seuraavat koko verkossa tapahtuvaa liikennettä ja havaitsevat epäilyttäviä paketteja analysoimalla protokollien aktiivisuutta. Päätelaitepohjaiset IPS-järjestelmät asennetaan päätelaitteelle, ja ne seuraavat pelkästään yhteen päätelaitteeseen kohdistuvaa liikennettä eivätkä koko verkkoa, kuten verkkopohjaiset.

6 VERTAILTAVAT PALOMUURITUOTTEET

6.1 VyOS 1.1.5

VyOS on Vyattan pohjalta syntynyt projekti. VyOS sai alkunsa vuonna 2013, kun Vyattan kehittäjä Brocade ilmoitti lopettavansa ilmaisen Vyatta Coren kehittämisen. VyOS on ilmainen Debian/GNU Linux -pohjainen avoimen lähdekoodin palomuuri- ja reititinohjelmisto, jonka voi asentaa fyysiseen palvelimeen tai virtuaalialustalle. VyOS:n uusin vakaa julkaisu on 1.1.5 (helium), ja se perustuu Vyatta Core 6.6 R1 -käyttöjärjestelmään. (Distrowatch 2014.)

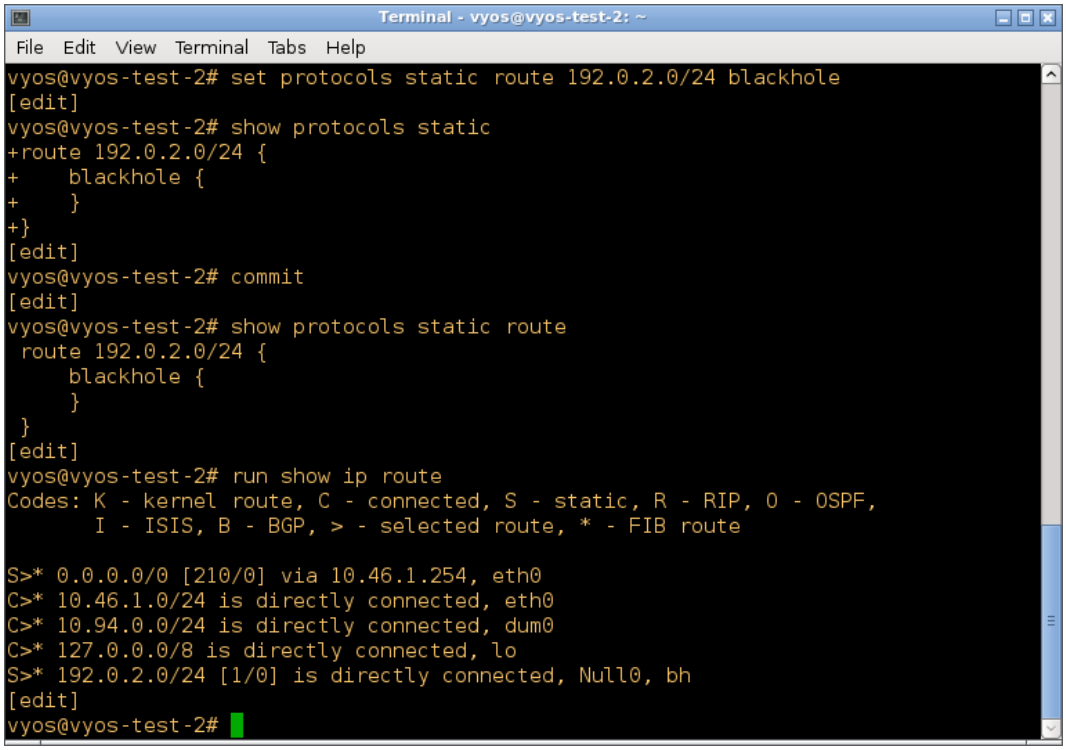
VyOS vaatii toimiakseen vähintään yhden Atom/C3-prosessorin, 512 MB RAM (random access memory) ja 2 GB tallennustilaa. Vaaditun prosessorin ominaisuuksien ja RAM:n määrä kasvaa sen myötä, mitä monimutkaisempia konfiguraatioita tekee. Esimerkiksi IPsec VPN -yhteydet vaativat prosessorilta laskentatehoa. VyOS:n pystyy asentamaan sekä fyysiselle että virtuaaliselle alustalle. Virtuaalialustoista tuettuja ovat KVM, Xen, VMWare ja Hyper-V. (The VyOS Project 2015.)

Paketinsuodatuksen VyOS:ssa hoitaa netfilter, samaan tapaan kuin useimmissa Linux-jakeluissa. Netfilterin avulla voidaan toteuttaa tilallinen tai tilaton paketinsuodatus ja NAT. Tavallisesta netfilteristä poiketen, VyOS:n palomuuri tukee palomuuriryhmiä (firewall group). Palomuuri-ryhmiin voidaan lisätä IP-osoitteita, verkkoja tai portteja. Palomuurisääntöjä luodessa voidaan ryhmiin viitata lähteenä tai kohteena. (The VyOS Project 2015.)

VyOS:ssa ei ole IDS:ää, sillä Vyatta Coresta poistettiin IDS versiossa 6.5 ja VyOS perustuu Vyatta Core versioon 6.6 R1. VyOS:n kehittäjien suunnitelmissa ei ole ainakaan vielä IDS:n lisääminen. (The VyOS Project 2015.)

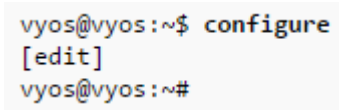
VyOS:ssa ei ole graafista käyttöliittymää vaan kaikki konfiguraatiot tehdään komentoliittymällä (The VyOS Project 2015.). Tämä tekee

VyOS:sta vaikeamman käyttää, kuin useat muut pk-yrityksille soveltuvat palomuuriohjelmistot.



KUVIO 11. VyOS CLI (The VyOS Project 2015)

VyOS:n CLI (Command-line Interface) (kuvio 11) eli komentoliittymällä on kaksi eri moodia: configuration mode ja operational mode. Operational modessa pystytään suorittamaan vain ylläpidollisia komentoja ja seuraamaan järjestelmän sekä palvelujen tilaa. Configuration mode sallii muutosten tekemisen järjestelmän konfiguraatioon. Käynnistyessä CLI on aina operational modessa. Operational moden tunnistaa kuviossa 10 olevasta $-merkistä. Komentoliittymään syötettäessä configure-komento siirrytään operational modesta configuration modeen. Samalla $-merkki vaihtuu #-merkiksi, joka tarkoittaa configuration modea (kuvio 12).



KUVIO 12. CLI configuration modeen siirtyminen (The VyOS Project 2015)

Configuration modessa kaikki muutokset aloitetaan set-komennolla, kuten kuviossa 13.

```
set nat source rule 100 outbound-interface 'eth0'
set nat source rule 100 source address '192.168.0.0/24'
set nat source rule 100 translation address 'masquerade'
```

KUVIO 13. NAT:n luominen (The VyOS Project 2015)

Konfiguraatioihin tehdyt muutokset otetaan käyttöön commit-komennolla ja tallennetaan save-komennolla. VyOS:n komentoliittymässä on komento commit-confirm <MINUTES>. Käytettäessä commit-confirm-komentoa voidaan varmistaa, että ei menetetä laitteen etähallintamahdollisuutta, vaikka tehdyt konfiguraatiomuutokset estäisivät yhteyden VyOS:iin. Commit-confirm-komennon antamisen jälkeen täytyy antaa erillinen confirm-komento, joka ottaa tehdyt muutokset käyttöön. Jos confirm-komentoa ei anneta 10 minuutin tai määritellyn ajan sisässä, VyOS käynnistää itsensä uudelleen ja ottaa käyttöön muutoksia edeltävän konfiguraatiotiedoston.

VyOS käyttää linux-jakeluista löytyvää tc:tä QoS:ssa. VyOS:n QoS-konfiguraatio tehdään kahdessa eri vaiheessa. Ensimmäisessä vaiheessa määritellään luokat (classes) tai jonot (queues) ja se miten verkkoliikenteen suodatin jakaa verkkoliikennettä niiden välillä. Toisessa vaiheessa määritellään ensimmäisessä vaiheessa luotu suodatuslinjaus verkkoliitännän ulospäin tai sisäänpäin suuntautuvalle liikenteelle (kuvio 14). (The VyOS Project 2015.)

```
set traffic-policy shaper WAN-OUT bandwidth '50Mbit'
set traffic-policy shaper WAN-OUT default bandwidth '50%'
set traffic-policy shaper WAN-OUT default ceiling '100%'
set traffic-policy shaper WAN-OUT default queue-type 'fair-queue'

set traffic-policy shaper LAN-OUT bandwidth '200Mbit'
set traffic-policy shaper LAN-OUT default bandwidth '50%'
set traffic-policy shaper LAN-OUT default ceiling '100%'
set traffic-policy shaper LAN-OUT default queue-type 'fair-queue'
```

KUVIO 14. QoS-esimerkki LAN- ja WAN-liitynnöille (The VyOS Project 2015)

VyOS pystyy toimimaan DHCP-serverinä ja tukee DHCP-relay-toimintoa. DHCP-relay otetaan käyttöön kuvion 15 komennoilla. VyOS:ssa on bugi, jonka vuoksi DHCP-relayta määriteltäessä täytyy määritellä verkkoliityntä, josta DHCP-serverin vastaukset tulevat. DHCP-serveri luodaan VyOS:ssa configuration modessa syöttämällä komento: set service dhcp-server shared-network-name <verkon nimi> subnet <aliverkon osoite/maski> start <alku ip> stop <loppu ip> (The VyOS Project 2015.)

```
set service dhcp-relay interface eth0
set service dhcp-relay interface eth1
set service dhcp-relay server 192.168.10.1
```

KUVIO 15. DHCP-relayn vaatimat komennot (The VyOS Project 2015)

VyOS tukee VPN-protokollista seuraavia: IPsec, SSL(OpenVPN), L2TP ja PPTP. Remote-access VPN käytössä edellä mainituista protokollista pystytään käyttämään SSL:ää, L2TP/IPsec:iä (L2TP over IPsec) ja PPTP:tä. Kuviossa 16 on esitetty, kuinka L2TP over IPsec konfiguroidaan remote-access VPN käyttöön VyOS:ssa. L2TP over IPsec toimii Windowsin ja Mac:n natiivien VPN-clienttien kanssa.

```
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec nat-traversal enable
set vpn ipsec nat-networks allowed-network 0.0.0.0/0

set vpn l2tp remote-access outside-address 203.0.113.2
set vpn l2tp remote-access client-ip-pool start 192.168.255.1
set vpn l2tp remote-access client-ip-pool stop 192.168.255.255
set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret
set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret <secret>
set vpn l2tp remote-access authentication mode local
set vpn l2tp remote-access authentication local-users username <username> password <password>
```

KUVIO 16. L2TP over IPsec konfiguraatio (The VyOS Project 2015)

6.2 pfSense 2.2.2

pfSense on ilmainen avoimen lähdekoodin palomuuri- ja reititinohjelmisto, jota kehittää Electric Sheep Fencing LLC. pfSense perustuu FreeBSD:hen

ja pfSensen kehittäminen aloitettiin m0n0wall-jakelun puutteiden takia. m0n0wall:ssa ohjelmiston käynnistyessä kaikki ladataan RAM-muistiin, eli mitään ei asenneta kovalevylle. Tämän takia m0n0wall:lla ei pystytty toteuttamaan kaikkia toimintoja, jotka vaaditaan nykyaikaiselta palomuurilta. (Buechler & Pingle 2009, 1.)

Useimmiten pfSenseä käytetään palomuurina erottamassa internetin sisäverkosta. Tämän lisäksi pfSenseä voidaan käyttää LAN- tai WAN-reitittimenä, langattoman verkon liityntäpisteenä, VPN-laitteena, DNS-palvelimena ja DHCP-palvelimena. (Buechler & Pingle 2009, 3 - 5.)

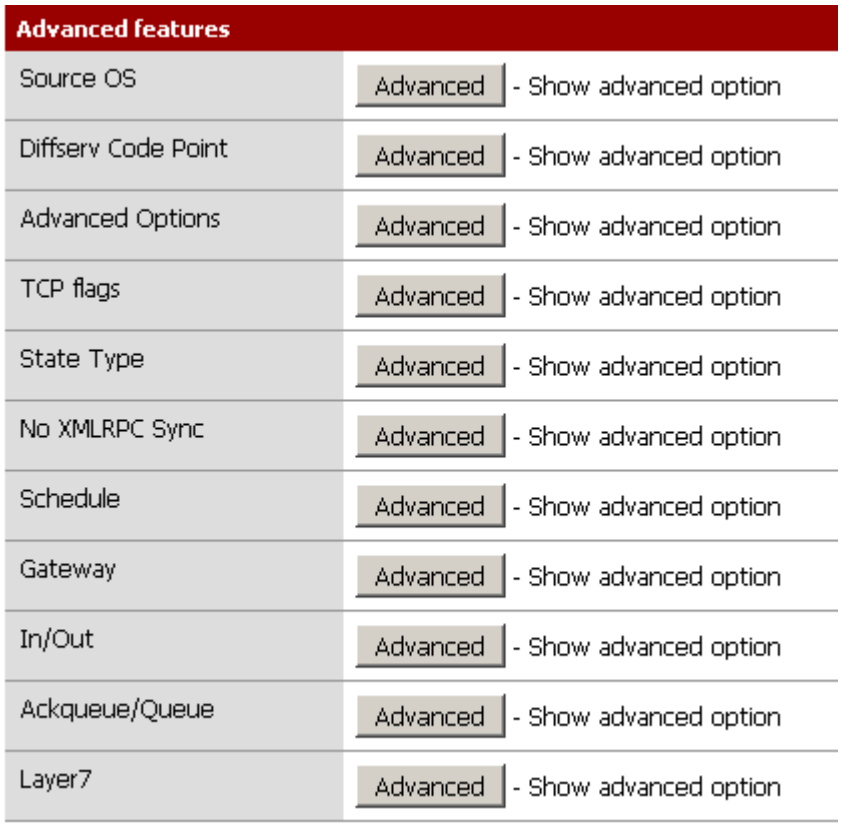
pfSense vaatii toimiakseen 100 MHz tai nopeamman prosessorin, 128 MB RAM:ia ja 1 GB tilaa kovalevyltä. Tällaisella laitteistolla saavutetaan noin 10 Mbps palomuurin suoritusteho. pfSensen palomuurin suoritusteho riippuu myös verkkokortin mallista. Halvat verkkokortit käyttävät paljon enemmän prosessori-tehoa, kuin korkeamman laatuiset verkkokortit. (Buechler & Pingle 2009, 21 - 22.)

pfSensen konfigurointi suoritetaan aina WebGUI:n (Web based Graphical User Interface) kautta, joten hallintaan pääsyä varten tarvitaan toinen PC (Personal Computer). Ensimmäistä kertaa avattaessa WebGUI avautuu aina asetusvelho. Asetusvelhon avulla suoritetaan pfSensen perus konfiguraatiot, kuten verkkoliitynnöiden IP-osoitteet, hostname, domain, dns-palvelimet, NTP-serverin valinta ja aikavyöhykkeen valinta. (Buechler & Pingle 2009, 55 - 62.)

pfSensen palomuurisäännöt löytyvät WebGUI:sta Firewall-valinnan takaa löytyvän Rules-valinnan alta. Sääntöjä voi tehdä kaikille määritellyille verkkoliitynnöille. pfSense estää WAN-liitännässä oletuksena RFC 1918 mukaiset yksityiset IP-alueet ja IANA:n (Internet Assigned Numbers Authority) määrittelemättömät ja varatut IP-osoitteet (kuvio 17).

KUVIO 17. Palomuurin oletussäännöt WAN-liitännälle (Buechler & Pingle 2009)

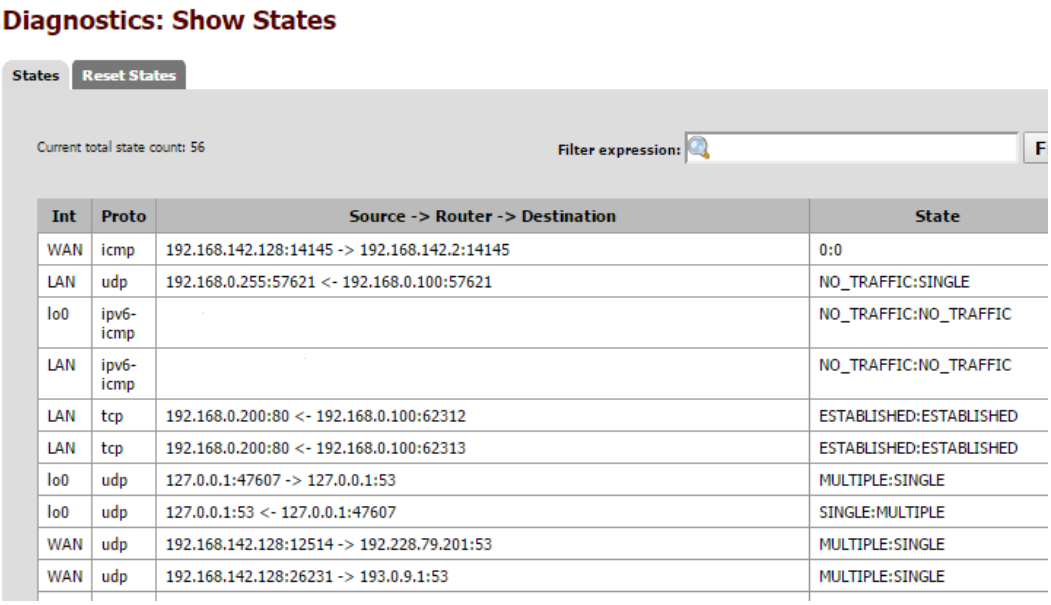
Tavallisten access-control-list-tyyppisten palomuurisääntöjen lisäksi pfSense tukee kehittyneitä palomuurisääntöjen ominaisuuksia. Näiden ominaisuuksien laajuudesta on esimerkki kuviossa 18.



KUVIO 18. Firewall Rules: Advanced features

pfSensen palomuuri on oletuksena tilallinen palomuuri. pfSensen tilallinen palomuuri pitää kirjaa yhteyksien avaamisista ja sulkemisista. Palomuurin tilatietoja pystyy tarkkailemaan joko WebGUI:n avulla (kuvio 19) tai

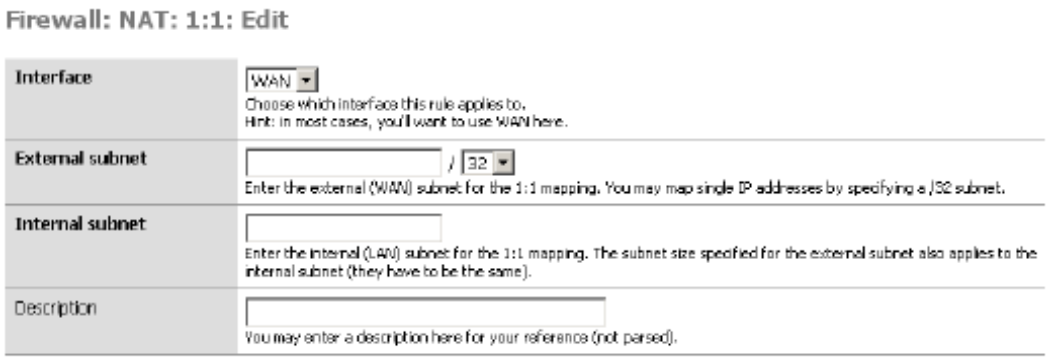
konsolista. Tallennettavien tilatietojen määrää pystyy muokkaamaan WebGUI:n avulla System > Advanced ja Firewall/NAT -välilehdeltä Firewall Maximum States. Jokainen tilatieto vie keskimäärin 1KB RAM:a. (pfSense 2015.)



Int	Proto	Source -> Router -> Destination	State
WAN	icmp	192.168.142.128:14145 -> 192.168.142.2:14145	0:0
LAN	udp	192.168.0.255:57621 <- 192.168.0.100:57621	NO_TRAFFIC:SINGLE
lo0	ipv6-icmp		NO_TRAFFIC:NO_TRAFFIC
LAN	ipv6-icmp		NO_TRAFFIC:NO_TRAFFIC
LAN	tcp	192.168.0.200:80 <- 192.168.0.100:62312	ESTABLISHED:ESTABLISHED
LAN	tcp	192.168.0.200:80 <- 192.168.0.100:62313	ESTABLISHED:ESTABLISHED
lo0	udp	127.0.0.1:47607 -> 127.0.0.1:53	MULTIPLE:SINGLE
lo0	udp	127.0.0.1:53 <- 127.0.0.1:47607	SINGLE:MULTIPLE
WAN	udp	192.168.142.128:12514 -> 192.228.79.201:53	MULTIPLE:SINGLE
WAN	udp	192.168.142.128:26231 -> 193.0.9.1:53	MULTIPLE:SINGLE

KUVIO 19. Palomuurin tilatiedot

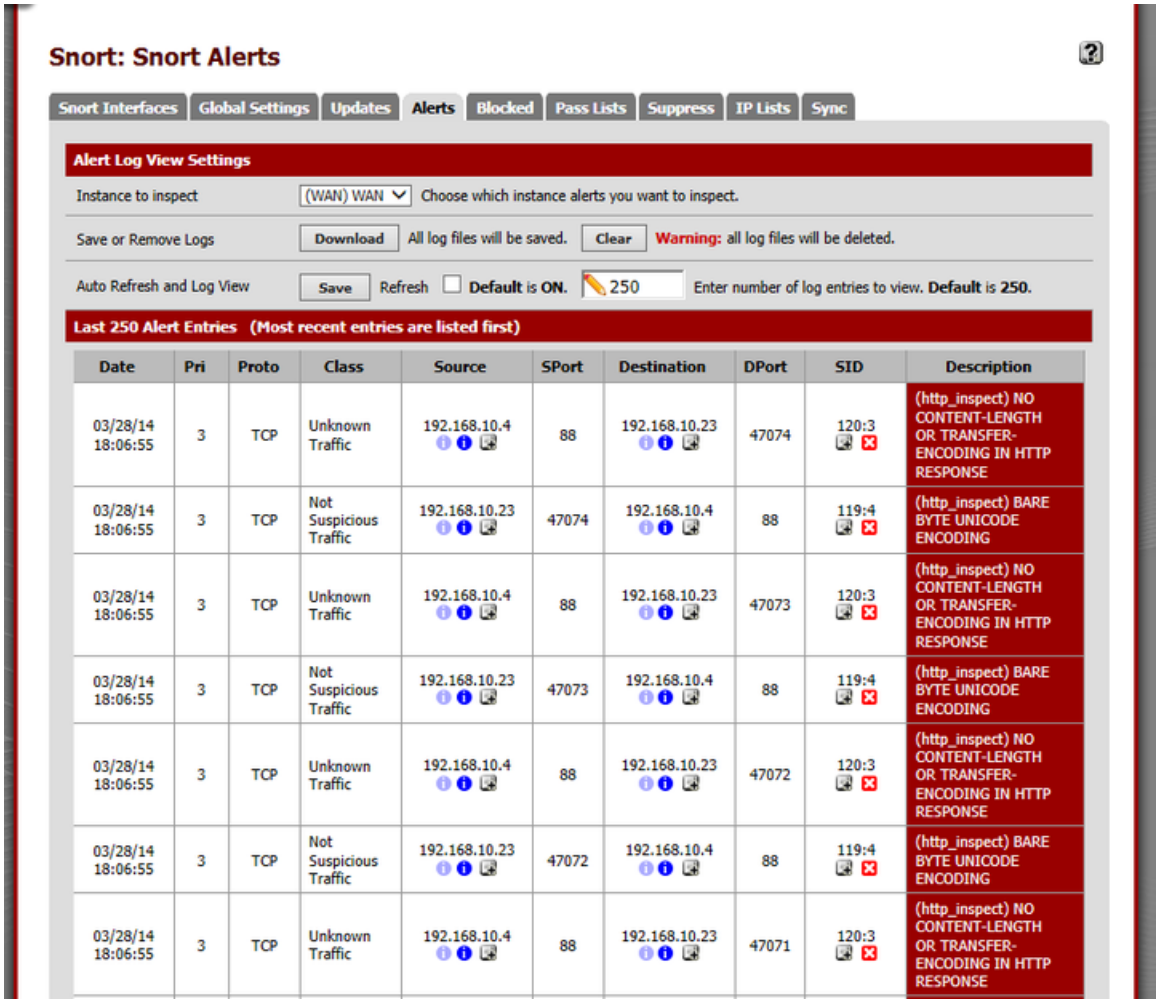
pfSense tukee useita eri NAT-tyyppejä. Kuviossa 20 esitetty 1:1 NAT:n eli staattisen NAT:n konfiguraatiosivu. Staattisen NAT:n suurin tietoturvariski on se, että palomuuri ei voi tietää, onko liikenne sallittaessa potentiaalisesti haitallista.



KUVIO 20. 1:1 NAT eli Staattinen NAT

Snort IDS -sovellus tulee pfSensen perusasennuksen mukana. Snort:n suurin ongelma on RAM-muistin käyttö. Snort konfiguraatiosta riippuen,

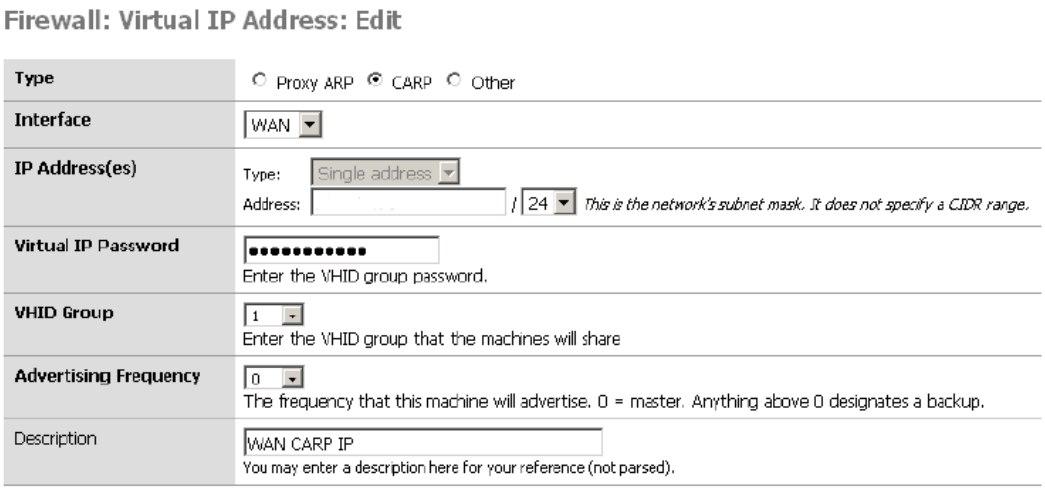
Snort:n vaatima RAM-muistin määrä voi nousta yli 1 GB:n. (Buechler & Pingle 2009, 25.)



KUVIO 21. Snort IDS:n hälytyksiä (pfSense 2015)

pfSensessä High Availabilityä varten on CARP (Common Address Redundancy Protocol) (kuvio 22), joka on BSD-pohjaisten käyttöjärjestelmien vastine VRRP:lle (Virtual Routing Redundancy Protocol). Pfsync on ohjelma, joka CARP-liityntää pitkin synkronoi palomuurin tilataulut primääriseltä palomuurilta sekundäärisille palomuureille. Tilatiedot lähetetään oletuksena multicast-tyyppisenä lähetyksenä, eli kaikki verkossa olijat vastaanottavat samat paketit. Tällä tavoin pfSense-laitteita voi olla varalla useampia. Vaihtoehtoisesti pfsynciin voidaan konfiguroida IP-osoite, jonka avulla pakotetaan synkronointi tapahtumaan vain kahden IP-osoitteen välillä. Pfsyncin ideana on saumaton vikasietoisuus, sillä tilataulujen ollessa samanlaiset

sekä primäärisessä että sekundäärisessä palomuurissa, pystyy sekundäärinen palomuuri ottamaan primäärisen palomuurin roolin ilman häiriöaikaa.

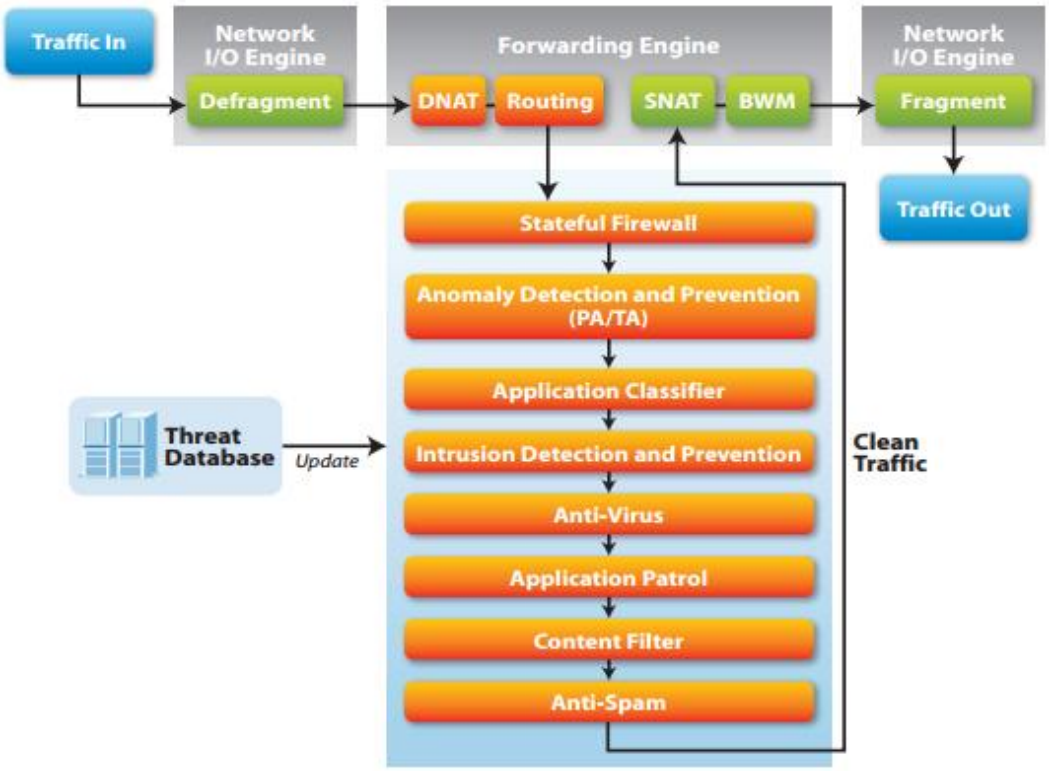


KUVIO 22. CARP-liitännän konfigurointi

6.3 Zyxel Zywall USG 300

Zyxelin Zywall USG 300 on Pk-yrityksille suunnattu valmis palomuuriratkaisu. Zywall USG 300 sisältää palomuurin, sisällön suodatuksen (kuvio 22), reititys- ja VPN-ominaisuudet.

USG 300 -mallin palomuuri on tilallinen palomuuri, johon voidaan yhdistää ACL-pääsylistat. Pääsylistoja pystyy kohdistamaan laitteen jokaiselle verkkoliitynnälle erikseen. USG 300:n tilallinenpalomuuri kykenee maksimissaan 350 Mbps läpisyöttöön. Käytettäessä Zyxelin virustorjuntaa ja IDP:tä (Intrusion Detection and Prevention) liikenteen läpisyöttö putoaa 80 megabittiin per sekunti. (Zyxel 2013.)



KUVIO 23. Zyxel USG 300 -palomuurin toimintaperiaate (Zyxel 2013)

Zywall USG 300:ssa on mukana BlueCoat- ja Commtouch-yritysten kehittämä sisällönsuodatus. Sisällönsuodatuksen avulla pystytään kontrolloimaan käyttäjien saatavilla olevia web-sivuja ja suodattamaan haittaohjelmia sähköpostiviesteistä. Web-sivuista voidaan suodattaa haitalliset sivustot ja haluttaessa muita sivustoja. (Zyxel 2013.)

VPN-tekniikoista Zyxel Zywall USG 300 tukee seuraavia:

- IPsec
- SSL
- L2TP.

USG 300 -laitteella pystytään muodostamaan site-to-site tyyppisiä-VPN tunneleita IPseciä ja L2TP:tä käyttäen. Samanaikaisten IPsec-tunnelien maksimimäärä on 200. Remote-access VPN on mahdollista ottaa käyttöön joko IPsecin tai SSL:n avulla. Remote-access IPsec VPN:ää käytettäessä tarvitaan käyttäjän päätelaitteeseen Zyxelin IPsec-asiakasohjelma, joka hoitaa yhdistämisen. Remote-access SSL VPN:ää käytettäessä USG 300

ei vaadi yhdistävältä päätelaitteelta erikseen asennettavaa asiakasohjelmaa, sillä USG 300 tukee Windowsin ja Mac:n sisäänrakennettuja VPN-asiakasohjelmia. (Zyxel 2013.)

6.4 Palomuurilaitteiden vertailu

VyOS-, pfSense- ja Zywall USG 300 -laitteiden vertailu keskenään on vaikeaa. Zywall on valmis paketti, ja sen ominaisuudet, kuten palomuurin suoritusteho, määräytyvät Zywall USG 300 -komponenttien perusteella ja USG 300:ssa niitä ei voi vaihtaa. pfSensen ja VyOS:n suoritusteho taas skaalautuu sen mukaan, miten tehokkaaseen palvelimeen ne asennetaan. Tämän vuoksi palomuuriratkaisuja vertailtiin vain vertailukelpoisten ominaisuuksien osalta. (Taulukko 1.)

Palomuuri	VyOS	pfSense	Zywall USG 300
Tilallinen palomuuri	Kyllä	Kyllä	Kyllä
Tilaton palomuuri	Kyllä	Kyllä	Kyllä
NAT-tuki	Kyllä	Kyllä	Kyllä
IDP	Ei	Kyllä (Snort)	Kyllä
QoS	Kyllä	Kyllä	Kyllä
DHCP	Server ja relay	Server ja relay	Server ja relay
VPN	Site-to-site IPsec, OpenVPN, L2TP/IPsec ja PPTP remote-access VPN	Site-to-site IPsec, OpenVPN, L2TP/IPsec ja PPTP remote-access VPN	Site-to-site IPsec ja SSL, remote-access IPsec/L2TP ja SSL remote-access
Sisällön suodatus	Saatavilla (squidGuard)	Saatavilla (squidGuard)	Kyllä
IPv6 tuki	Kyllä	Kyllä	Kyllä
High availability (HA)	Kyllä	Kyllä	Kyllä
CLI	Kyllä	Ei	Kyllä
GUI	Ei	WebGUI	WebGUI

TAULUKKO 1. Laitteiden vertailu

Kaikissa kolmessa vertaillussa laitteessa on tilallisen palomuurin lisäksi tilaton palomuuri. Source NAT ja destination NAT osoitteenmuunnoksien lisäksi jokainen laite tukee staattista NAT:a ja PAT:a (Port Address Translation).

Vertailluista laitteista VyOS ei tue tällä hetkellä minkäänlaista IDP-järjestelmää. Zywall USG 300:ssa on Zyxelin oma Intrusion Detection and Prevention System ja pfSenseen on saatavilla avoimen lähdekoodin Snort IDP -ohjelmisto.

Quality Of Service-ominaisuudet ovat kaikissa vertailun laitteissa yhtä monipuoliset. pfSense käyttää FreeBSD:n ALTQ network scheduleria ja VyOS käyttää Linux-käyttöjärjestelmien traffic control -nimistä network scheduleria, joka on osa iproute2-pakettia. Zywall USG 300 käyttää ZLD-ohjelmistonsa QoS-ominaisuutta kaistanrajoitukseen ja pakettien hallintaan.

Site-to-site VPN:n toteuttaminen onnistuu IPsec:n avulla kaikilla vertailluilla laitteilla. pfSense ja VyOS tarjoavat mahdollisuuden käyttää L2TP over IPsec:iä site-to-site-tunnelin muodostamiseen. Zywall USG 300 ei tue L2TP:tä site-to-site ratkaisuissa, mutta USG 300 kykenee muodostamaan site-to-site tyyppisen tunnelin käyttäen SSL-protokollaa. Remote-access VPN ominaisuudet ovat vertailluissa laitteissa yhtä laajat. Zywall USG 300 on vertailun ainoa laite, jolla tietoturvallinen remote-access VPN ei vaadi erikseen asennettavaa asiakasohjelmaa. VyOS:n ja pfSensen avulla pystytään myös muodostamaan remote-access VPN-yhteyden ilman erillistä asiakasohjelmaa, mutta silloin täytyy käyttää PPTP-protokollaa. PPTP-protokolla ei ole nykypäivänä enää tietoturvallinen, paitsi käytettäessä EAP-TLS autentikaatioprotokollaa. EAP-TLS vaatii taas täyden PKI-infrastruktuurin. (Public Key Infrastructure)

Zyxel Zywall USG 300:n sisällönsuodatusominaisuudet ovat kolmikon kehittyneimmät. USG 300 pystyy suodattamaan web-sivujen lisäksi sähköposteja. VyOS:ssa ja pfSensessä sisällönsuodatuksen suorittaa Squid 3-proxyn lisäosa SquidGuard. SquidGuard ei kykene email-

suodatukseen. Oletusasetuksilla SquidGuardin mukana ei tule kunnon estolistaa, vaan ne täytyy ladata erikseen.

High Availability -ominaisuudet ovat erittäin hyvät kaikissa laitteissa. VyOS tukee VRRP:tä (Virtual Router Redundancy Protocol). VRRP:n kautta kaksi VyOS-laitetta kykenevät muodostamaan klusterin ja synkronoimaan asetustiedot keskenään. pfSense tukee BSD-pohjaisille jakeluille tyypillisesti CARP:ia (Common Address Redundancy Protocol). CARP:n avulla kaksi pfSense-laitetta pystyvät muodostamaan klusterin ja synkronoimaan asetustiedot, aivan kuten VyOS VRRP:n avulla. VRRP:n ja CARP:n avulla luodut klusterit lisäävät palomuuriratkaisun vikasietoisuutta, sillä yhden laitteen vikaantuessa toinen jatkaa toimintaansa. Zyxel Zywall USG 300:ssä voidaan konfiguroida useampia WAN-portteja, jolloin verkkoliikennekuorma jakautuu porttien välille. USG 300 tukee myös klusterointia, jonka avulla saavutetaan vastaavanlainen vikasietoisuus kuin pfSensen ja VyOS:n klusteroinnilla. Kaikki kolme laitetta tukevat myös backup-WAN:a eli varaliittymää, joka tulee käyttöön, kun pääasiallinen WAN-yhteys vikaantuu.

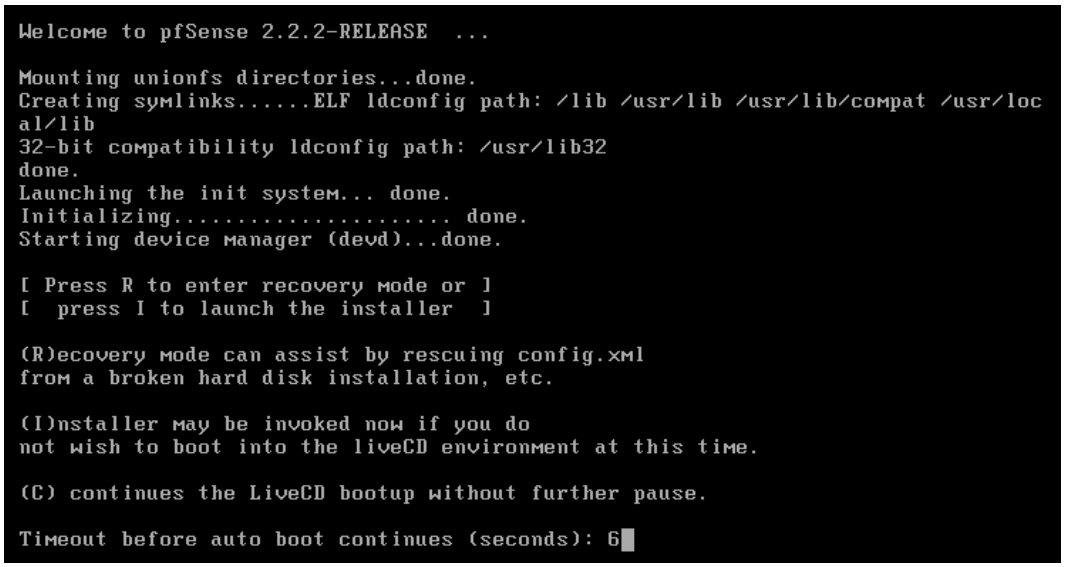
pfSensessä ei ole ollenkaan omaa komentoliittymää asetusten muuttamiseen, vaan kaikki muutokset tehdään graafisen web-liittymän kautta. VyOS taas ei sisällä ollenkaan minkäänlaista graafista käyttöliittymää, joten kaikki muokkaukset tehdään CLI:n kautta. Zywall USG 300 sisältää sekä CLI:n että web-liittymän muutoksien tekemistä varten.

pfSense ja Zywall USG 300 ovat molemmat hyviä palomuureja pk-yritykselle, sillä niissä on kaikki verkon turvaamiseen vaadittavat ominaisuudet. VyOS:n suurin puute IDS:n lisäksi on graafisen käyttöliittymän puuttuminen, mikä tekee siitä vaikeamman käyttää. VyOS:n komentoliittymä vaatii myöskin opettelua.

7 PFSENSEN KÄYTTÖÖNOTTO

7.1 pfSensen asennus

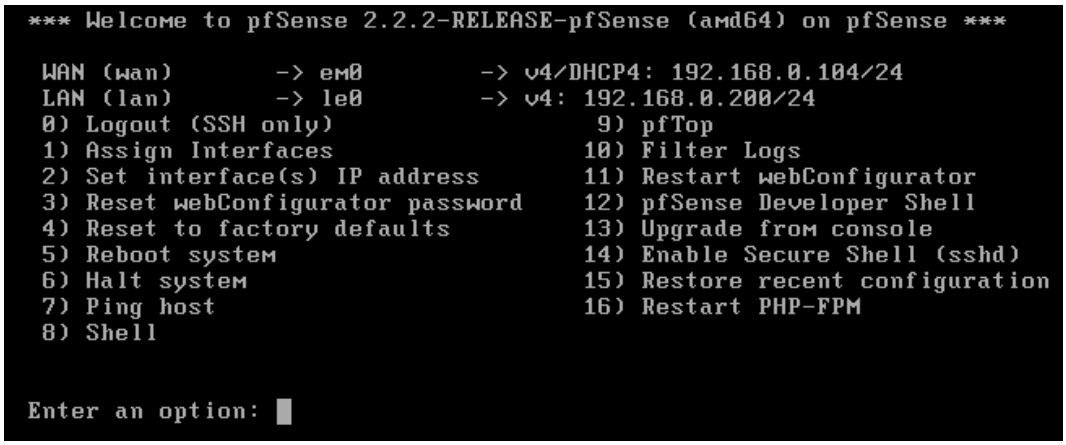
Tässä työssä pfSense asennettiin IBM X3550 M3 -palvelimeen joka oli varustettu kahdeksalla verkkokortilla. Verkkokorteihin konfiguroitiin WAN- ja LAN-liityntöjen lisäksi vierasverkko, josta pääsi pelkästään internetiin ja CARP-liityntä. CARP-liitynnän avulla kahdennettaisiin palomuuri, jos kahdentaminen todetaan tarpeisiin sopivaksi ratkaisuksi. pfSensen asennus on yksinkertainen prosessi. pfSensen asennus vaatii ainoastaan asennusmedian ja palvelimen, johon pfSense asennetaan. pfSenseä ei ole pakko asentaa palvelimelle ensimmäisellä käyttökerralla, vaan sitä pystyy kokeilemaan LiveCD-tyyppisesti suoraan asennusmedialta (kuvio 24).



KUVIO 24. pfSensen asennus

Asennusohjelman käynnistyttyä voi valita quick-installin, joka asentaa pfSensen ilman kysymyksiä. Asennusohjelman päätyttyä palvelin käynnistetään uudestaan, määritellään WAN- ja LAN-liitynnät, pfSense on valmiina käytettäväksi. pfSensestä puuttuvan CLI:n takia palvelimella näkyy ainoastaan valikko, jonka avulla pystyy suorittamaan vain ylläpidollisia toimenpiteitä (kuvio 25). Ensimmäistä kertaa kirjauduttaessa

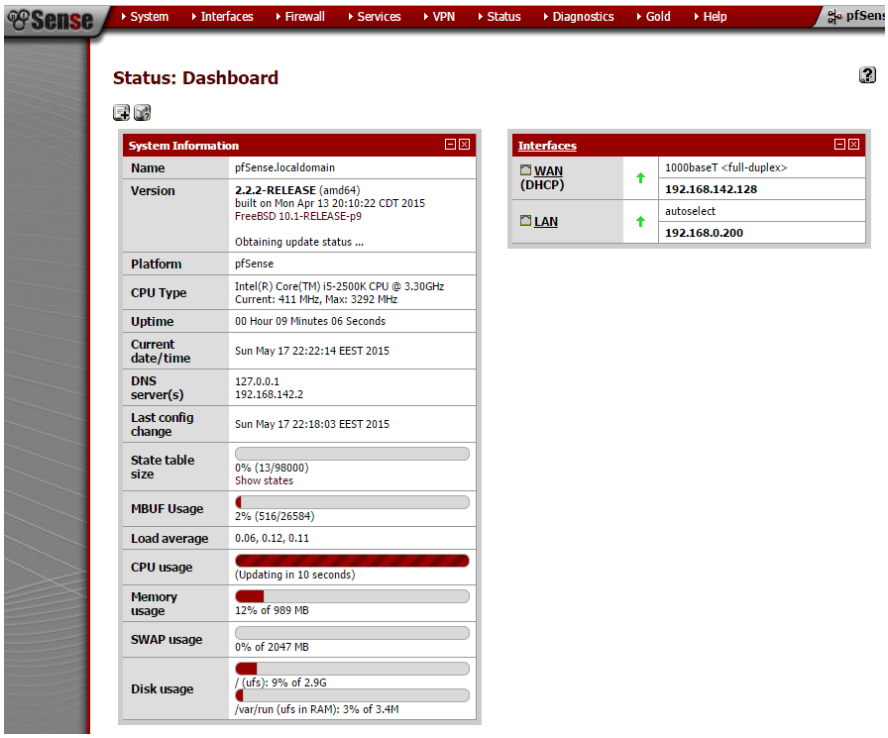
pfSensen web-käyttöliittymään tulee asennusvelho, jonka pyytämät asetukset säätämällä saadaan pfSense toimintakuntoon.



KUVIO 25. pfSensen ylläpitovalikko

7.2 pfSensen hallinta WebGUI:n avulla

pfSensen hallinta tapahtuu WebGUI:n avulla (kuvio 26). Kirjauduttaessa sisään WebGUI:hin kaikki ominaisuudet on loogisesti järjestetty valikkoihin aiheittain. Valikoista tärkeimmät palomuurin toimintakuntoon saattamisen kannalta ovat Interfaces- ja Firewall-valikot. Interfaces-valikon alta konfiguroidaan liitynnöille IP-osoitteet.



KUVIO 26. pfSense Dashboard

Kun palomuuri on saatettu toimintakuntoon, tärkein valikko on Diagnostics (kuvio 27). Diagnostics-valikon alta löytyvät kaikki pfSensen diagnostiikka-ominaisuudet. Näistä olennaisimmat ovat palomuurin tilatietojen seuraamiseen tarkoitetut States ja States Summary.

KUVIO 27. pfSensen diagnostiikka-ominaisuudet

7.3 Käyttöönoton hyödyt

Ottamalla pfSense käyttöön tavoiteltiin helposti hallittavaa palomuuria pk-yrityksen vanhan iptables- ja netfilter-pohjaisen palomuurin tilalle. Tarkoituksena oli saada käyttöön palomuuri, jota pystyy hallitsemaan graafisesti ja ilman linux- tai unix-osaamista.

Iptables-pohjaiseen palomuuriin verrattuna pfSensen käyttöönoton jälkeen pk-yrityksen palomuurin hallinnasta pystyy suoriutumaan lähes kuka tahansa palomuurin ja palomuurin sääntöjen toiminnasta ymmärtävä henkilö. pfSensen palomuurin sääntöjen muokkaaminen ja tilatietojen seuraaminen on graafisen käyttöliittymän kautta paljon helpompaa, kuin komentoliittymästä iptables:n käyttäminen. pfSensen helpon hallinnan

vuoksi pk-yritykselle pystytään luomaan tilallinen tai tilaton palomuuri, ilman linux- tai unix-osaamista.

8 YHTEENVETO

Tässä opinnäytetyössä tutustuttiin pk-yrityksille sopivien palomuurien ominaisuuksiin ja niiden toimintaan. Tutkimusosassa kerrottiin ensin pk-yrityksen tietoturvan tarpeellisuudesta ja suurimmista ongelmista. Sen jälkeen kerrottiin palomuurien ominaisuuksista ja niiden toiminnasta, painottaen VPN-yhteyksiä.

Käytännön osuudessa tutkittiin kahta palomuuriohjelmistoa, pfSenseä ja VyOS:ia, sekä valmista palomuurilaitetta, Zyxell Zywall USG 300:aa ja vertailtiin niiden ominaisuuksia. Käytännön osuudessa oli tarkoitus selvittää, minkälainen on paras mahdollinen palomuuri pk-yritykselle, pitäen mielessä palomuurin helppokäyttöisyyden. pfSensen käyttöönottoon perehdyttiin käytännön osuudessa.

Jokaisessa vertaillussa laitteessa oli lähes vastaavanlaiset ominaisuudet. VyOS ei sisältänyt minkäänlaista tukea Intrusion Detection and Prevention Systemiä (IDPS) eikä graafista käyttöliittymää. Muuten laitteista löytyi kaikki ominaisuudet, mitä pk-yritys voi palomuuriltaan haluta.

Vertailluista laitteista Zyxell Zywall USG 300 ja pfSense ovat sopivia pk-yritykselle niiden suhteellisen helpon käyttöönoton ja konfiguroinnin takia. pfSense tulisi valita, jos yrityksen vaatimukset palomuurille kasvavat lähitulevaisuudessa oletettavasti. Zywall USG 300 oli vertailun helppo käyttöisin, mutta USG 300:n suorituskyky on rajallinen ja sitä ei ole mahdollista nostaa päivittämällä komponentteja. VyOS:ää voi suositella vain sellaiselle pk-yritykselle, jolla on IT-osasto, jolla on kokemusta erilaisista kaupallisista palomuurituotteista.

Vertailluista palomuureista voidaan olettaa VyOS:n kehittyvän samalle tasolle, kuin pfSense ja olemaan täten varteenotettava vaihtoehto valittaessa palomuuriratkaisua pk-yritykselle. VyOS ja pfSense saavat mahdollisesti lisää ominaisuuksia tulevissa päivityksissä, mutta Zywall USG 300:n kohdalla se on epätodennäköisempää.

Tulevaisuudessa pk-yrityksissä palomuurin tärkeys tulee korostumaan, sillä SaaS (Software as a service) -tyyppiset pilvipalveluratkaisut yleistyvät kovaa vauhtia. Pilvipalvelujen yleistymisen lisäksi kyberrikollisuus kasvaa huomattavaa vauhtia, jolloin palomuurien ja tietoturvan merkitys pk-yrityksissä kasvaa entisestään.

LÄHTEET

Buechler, C. & Pingle, J. 2009. pfSense: The Definitive Guide: The Definitive Guide to the pfSense Open Source Firewall and Router Distribution. USA: Reed Media Services.

Carrel, D. & Harkins, D. 1998. RFC 2409 [viitattu 14.5.2015]. The Internet Society. Saatavissa: http://tools.ietf.org/html/rfc2409

Check Point. 2005. Stateful Inspection Technology [viitattu 13.5.2015]. Check Point Software Technologies Ltd. Saatavissa: https://www.checkpoint.com/download/public-files/Stateful_Inspection.pdf

Check Point. 2013. The Attacker's Target: The Small Business [viitattu 13.5.2015]. Check Point Software Technologies Ltd. Saatavissa: http://www.checkpoint.com/downloads/product-related/whitepapers/SMB_Whitepaper.pdf

Cisco. 2009. SSL VPN [viitattu: 14.5.2015]. Saatavissa: http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t11/htwebvpn.html#wp1053815

Cisco. 2015. Network Security for Small Business [viitattu 12.5.2015]. Cisco Systems. Saatavissa: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/network_security_considerations/index.html

Curell, G. 2014. Create DHCP Server in VyOS [viitattu 15.5.2015]. Saatavissa: http://grantcurell.com/2014/07/08/create-dhcp-server-in-vyos/

Dell Software. 2013. Why switch from IPSec to SSL VPN [viitattu 13.5.2015]. Dell Software. Saatavissa: http://www.sonicwall.com/downloads/EB_Why_Switch_from_IPSec_to_SSL_VPN.pdf

Distrowatch. 2014. VyOS [viitattu 14.5.2015]. Saatavissa: http://distrowatch.com/table.php?distribution=vyos

Frahim, J., Santos, O. & Ossipov, A. 2014 Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services, Third Edition. Indianapolis: Cisco Press.

Kaufman, E. 2005. RFC 4306 [viitattu 13.5.2015]. The Internet Society. Saatavissa: http://tools.ietf.org/html/rfc4306

Komar, B., Beekelaar, R. & Wettern, J. 2003. Firewalls For Dummies, Second Edition. Indianapolis: Wiley Publishing.

Microsoft. 2003. What is DHCP? [viitattu 15.5.2015]. Saatavissa: https://technet.microsoft.com/en-us/library/cc781008%28v=ws.10%29.aspx

pfSense. 2015. pfSense Documentation [viitattu 15.5.2015]. Saatavissa: https://doc.pfsense.org/

Strebe, M. & Perkins, C. 2002 Firewalls 24seven. Alameda: Sybex.

The VyOS Project. 2015. VyOS Wiki [viitattu 14.5.2015]. Saatavissa: http://vyos.net/wiki/Main_Page

Yle. 2015. Kyberrikollisuus moninkertaistunut – yli puolet rikoksista jää selvittämättä [viitattu 11.5.2015]. Yleisradio Oy Saatavissa: http://yle.fi/uutiset/kyberrikollisuus_moninkertaistunut__yli_puolet_rikoksista_jaa_selvittamatta/7809103

Zyxel. 2013. ZyWALL USG 300 Datasheet [viitattu 15.5.2015] Saatavissa: ftp://ftp2.zyxel.com/ZyWALL_USG_300/datasheet/ZyWALL%20USG%20300_9.pdf